Low Power Wide Area Network (LPWAN) Technologies for Industrial IoT Applications

NIKOLAOS TSAVALOS
AHMAD ABU HASHEM
MASTER´S THESIS
DEPARTMENT OF ELECTRICAL AND INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING | LTH | LUND UNIVERSITY

Master's Thesis

with title:

Low Power Wide Area Network (LPWAN) Technologies for Industrial IoT Applications

written by:

Nikolaos Tsavalos & Ahmad Abu Hashem

supervised by:

Stefan Höst & Jens Jakobsen

Department of Electrical and Information Technology

Faculty of Engineering, LTH, Lund University

SE-221 00 Lund, Sweden

June 2018

Abstract

Industrial Internet of Things (IIoT) is part of the well-known IoT concept where a large number of devices need to be interconnected in order to collect and exchange data. Companies' aim is not only to minimize cost during product design, operation and maintenance but also to enable remote monitoring on the efficiency of the devices-assets through the utilization of cloud services. Low Power Wide Area Network (LPWAN) is seen as one of the enablers for IoT and can be realized by implementing emerging technologies such as Sigfox, LoRaWAN, NB-IoT and CAT-M1. The aim of this thesis is to define which technology is the most suitable for a vast range of applications. In the second and third chapters, an in-depth analysis and theoretical comparison of these technologies regarding frequency bands, data rate, power consumption, coverage, quality of service, latency, mobility, and cost is provided. However, based on this comparison, it is apparent that there is not a single technology that can satisfy all different requirements and needs. Therefore, applications such as smart metering, network monitoring, manufacturing, supply chain tracking, agriculture or power generator monitoring can take advantage of some technologies more than others and this is shown in the third chapter. As far as the practical part of this thesis project is concerned, we chose to test Sigfox in the area of Skåne for reasons that are explained in the fourth chapter. Using Lopy4, a module provided by Pycom, we performed field measurements in outdoor, indoor, rural and urban scenarios. Results concerning coverage, outage capacity, range, and latency are extracted in the fourth chapter and further commented in the fifth chapter. Finally, in the sixth chapter, future work suggestions and insights are given by the authors.

Acknowledgements

Firstly, we would like to thank our supervisors, Stefan Höst and Jens Jakobsen for their assistance and guidance throughout this five-month academic journey. Without their constructive suggestions and comments, we would not be able to complete this project in time.

Secondly, the completion of this master thesis signifies also the end of our studies at Lund University and we would like to express our warm gratitude to all the professors that imparted their knowledge, experience and insights to us.

Last but not least, we would like to thank our families for supporting us during these two years of living and studying abroad and we would like to dedicate this work to them.

Popular Science Summary

The best choice is not always the perfect choice in life. You might need sometimes to take the most suitable choice which is corresponding to the needs instead. That is also the result we get from our work, in which we compare four technologies that are used to enable communication between machines in long distance, carrying small amount of data.

In daily life, wireless communication is well-known as either WI-FI or cellular connection. WI-FI, for instance, allows receiving a huge amount of data wirelessly like watching a movie or downloading a game, within a local area (i.e. a home or a library), for low costs (i.e.the price of modem and monthly fee). Even cellular communication allows the same large amount of data but within a larger area and for higher costs (i.e. the price of mobile and a monthly fee based on how much data is used). Nowadays, cities are changing to smart cities. It is not the persons who connect each other but it is machine to machine connections (i.e. a garage door opens when your car is nearby, a counter which calculates the free places in a parking lot or small chip that sends the location of your pet repeatedly to your mobile phone). These services require technologies different than WI-FI or cellular.

Low power wide area (LPWA) technologies appear to enable the deployment of such services. In this thesis, four technologies, Sigfox, LoRa, NB-IoT, and CAT-M1 are theoretically compared aiming to find the most suitable for the future of Internet of Things (IoT). Soon, one realizes that it is not about an apple to apple comparison since each technology has properties that serve different customers/needs. After presenting the fundamental properties of each technology (as it is shown in the second and third chapter), the conclusion that there is not a single winner but all of them are suitable for different applications, is coming to surface. In health-care services where data about health is transmitted to monitors, CAT-M1 is a more suitable choice than others because of its fast reaction and low-latency. In agriculture, where data about soil PH and water usage indicators are transmitted, Sigfox and LoRaWAN are more suitable technologies because of their cost-efficiency and low bandwidth usage.

The aim of this thesis, is to validate the theoretical results for the most prominent technology, which is decided to be Sigfox for the purpose of this work. Using a module that consists of a chip and an antenna, we study how coverage changes depending on whether the module is located in a rural or urban area. Furthermore, except for outdoor scenarios, indoor cases are evaluated in order to understand the technology's performance in places where there are a lot of walls, obstacles or basement. The results from the practical implementation analysis are interesting and are being discussed in the last part of this work.

TABLE OF CONTENTS

Chapter 1. Introduction 13

1.1 Background 13

1.2. Problem Definition/Motivation 14

1.3. Previous Work 15

1.4. Approach 16

1.5. Organization of Thesis 17

Chapter 2. Technologies 19

2.1. Sigfox 19

2.1.1. Introduction 19

2.1.2. Technology 19

2.1.3. Network Architecture 22

2.1.4. Security 23

2.2 LoRaWAN 25

2.2.1. Introduction 25

2.2.2. Technology 26

2.2.3. Network architecture 31

2.2.4. Security 33

2.3. Narrow-Band IoT 35

2.3.1. Introduction 35

2.3.2. Technology 36

2.3.3. Network Architecture 40

2.3.4. Security 43

2.4. CAT-M1 46

2.4.1. Introduction 46

2.4.2. Technology 46

2.4.3. Network Architecture 48
2.4.4. Security 49
Chapter 3. Theoretical Comparison 51
3.1 Introduction 51
3.2. Frequency bands and data rate 51
3.3. Power consumption and Coverage 52
3.4. Quality of Service 54
3.5. Latency 55
3.6. Mobility 55
3.7. Cost 56
3.7.1 Module Cost 56
3.7.2 Network Cost 56
3.7.3 Availability 58
3.8. Applications 59
3.8.1. Smart Metering Applications 59
3.8.2 Network Monitoring Applications 60
3.8.3. Applications in Manufacturing Sector 60
3.8.4. Supply Chain Tracking Applications 60
3.8.5. Agriculture Applications 61
3.8.6. Power Generator Monitoring 61
Chapter 4. Practical Implementation 63
4.1. Selection Approach 63
4.1.1. Introduction 63
4.1.2. Choosing Sigfox 64
4.2 Measurement Methodology 65
4.2.1 Equipment Overview 65
4.2.2 Scenarios Overview 66
4.3 Results 70

Chapter 5. Conclusion 75
Chapter 6. Future Work 77
References 81
Appendix A 85
A.1 Main.py 85
A.2 Boot.py 85

Chapter 1. Introduction

1.1 Background

Industrial Internet of Things (IIoT) is part of the well-known IoT concept where a large number of devices need to be interconnected in order to collect and exchange data. Companies' aim is not only to minimize cost during product design, operation, and maintenance but also to enable remote monitoring on the efficiency of the devices-assets through the utilization of cloud services.

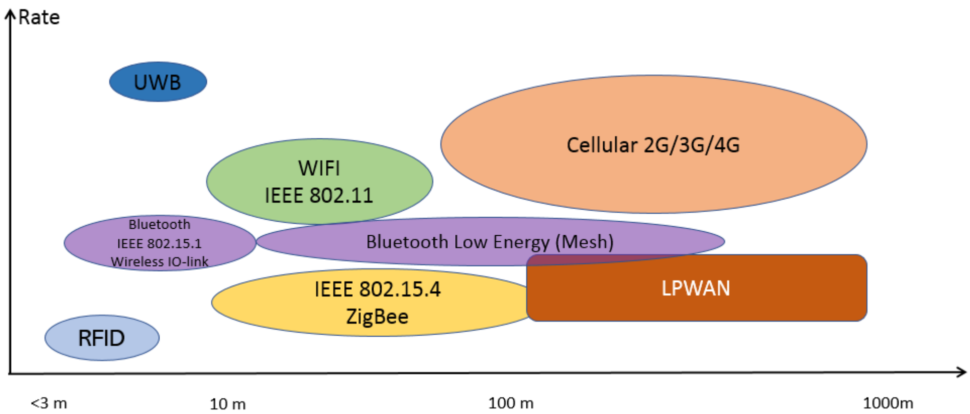

Figure 1.1. Coverage and Transmission Rate (bps) Comparison among Wireless Technologies

Low Power Wide Area Network (LPWAN) is seen as one of the enablers for Internet of Things (IoT) where billions of devices will be connected as mentioned above. In addition to the existing short-range wireless systems using technologies such as Bluetooth, Zig-Bee, WIFI, etc. LPWA networks offer wide area coverage for numerous IoT applications that require low power [1]. As a consequence, due to its low-cost operation, compared to the traditional mobile network systems, and to its better power efficiency, it can be considered as the future solution in Industrial IoT. In Figure 1.1 [2], a comparison is shown between short range and long range wireless technologies regarding transmission rates.

As stated above, LPWAN can be realized by implementing emerging technologies such as Sigfox, Lora, NB-IoT, and CAT-M1. All these technologies licensed or not, proprietary or nonproprietary are presented in [3] and can be used a different solution for the clear majority of Industrial IoT.

1.2. Problem Definition/Motivation

Regarding the motivation for this thesis project, numerous applications involve smart metering and monitoring services. Parameters such as temperature, geolocation, humidity, power levels, gas level etc. can be of great importance for the overall good maintenance and performance of a system. For example, such an application is inspired by *HMS Industrial Networks* and is focused on *Diesel tank monitoring*. A wireless communication gateway is connected to the Diesel tank and it transmits data to a cloud-based server where all parameters can be monitored in real-time. It is extremely important to be aware of the levels of Diesel tanks in order to avoid unnecessary transports for a fill-up or to enable alerts in case of appearing operational risks [4]. Therefore, this thesis is focused mainly on this type of applications where there is no need to transmit very frequently to the cloud server (diesel tank levels do not change every 10 seconds for instance). However, through this thesis, a holistic view regarding the large range of possible applications is maintained, where there is a need for constant transmission and real-time handling (monitoring the temperature to prevent explosions and to react as soon as possible if not immediately).

It is a very challenging task to decide on which wireless technology is the best fit for such an application because a lot of parameters and trade-offs have to be taken into consideration. Is cost-efficiency more important than quality of service? Can there exist a balance between reliable performance and latency? These are just a few questions that have to be answered and investigated by design engineers when facing such decisions. However, this is only one of the large number of applications that LPWA technologies promise to serve as Industrial IoT grows. Other applications may involve a high need for mobility scenarios, deep indoor coverage or even real-time notifications. Therefore, to make a fast estimation on which technology needs to be used, can turn out to be bold eventually.

1.3. Previous Work

In this thesis, many scientific papers and research material have been utilized. Many papers have been published, most of them include field measurements of one technology, or maybe a comparison between two technologies with respect to some of the aspects and parameters that we are interested in. Therefore, we had to study and collect the database we needed from many scientific-trusted resources. Sometimes we made a direct contact with the authors of papers to discuss the methodology and results they got with them.

“Interference impact on Coverage and Capacity in Low Power Wide Area IoT Networks” [5] and “Coverage comparison of GPRS, NB-IoT, LoRa and Sigfox in 7800 km^2 area” [6] are two scientific papers written by a group of six researchers working in Aalborg University in cooperation with Telenor commercial network and published in IEEE in November 2017. The papers compare the coverage of four IoT technologies in different scenarios, including rural and urban areas over 27000 km^2. The impact of interference on coverage has been also studied. These papers are used as a reference to compare the coverage limits of the technologies in focus. As additional support, we contacted Mads Lauridsen who is one of the authors of the papers.

“Narrow Band Internet of things” [7] is a resource describing detailed NB-IoT’s technical aspects, network architecture, some of NB-IoT applications and Network security. The papers are written by two senior members in IEEE and published in September 2017.

A good comparison between LoRa and NB-IoT is provided by “A survey on LPWA technology: Lora and NB-IoT” [8]. These papers are written by researchers in Electronics and Electrical Engineering department at Dongguk University, Seul. Besides to the comparison between two technologies, the papers also provide information about the rollout of the technologies in East Asia.

In this thesis, we introduce a comparison between four technologies, some of them are still under rollouts, such as Sigfox and CAT-M1. That is why only few documentation could be found. Sources, in this case, were the technology’s providers and their online website such as LoRa Alliance and Sigfox.

1.4. Approach

The goal of this thesis work is to analyze Sigfox, LoRa, CAT-M1, and NB-IoT technologies in terms of suitability for Industrial IoT. In addition, it is desired that a practical implementation is carried out with one selected technology. This practical implementation includes a lot of measurement sets, each one for a specific purpose. For example, the measurements are divided into urban and rural scenarios, or even in indoor and outdoor cases in order to show how performance is affected by deep penetration losses or obstructs. The aim of this test is to compare the theoretical knowledge with the actual findings from the performed measurements. Implementing all four technologies would be unrealistic (timewise) regarding the timeframe of this Master thesis. Therefore, the main challenge is to decide a priori which technology is the most suitable for implementation. This decision is very challenging and is dependent on many parameters. Parameters that we will initially focus on, in the theoretical section, are coverage, range, cost, bandwidth, energy efficiency, frequency bands, regulations, interference, capacity, mobility etc. Tables and graphs regarding the comparison of all these parameters are included in the theoretical comparison section of this Master thesis report.

Our main challenge is to research as much as we can on the four proposed technologies during the first month of the timeline and afterward to decide which technology will be implemented for the practical realization of our Master thesis project because we understand that the implementation part can be time-consuming. This Master thesis work is divided into three main stages:

1.Study of scientific papers or related articles that include useful information about Industrial IoT, LPWAN, LoRa, Sigfox, NB-IoT, and CAT-M1. These papers can be found on the references table.

2. Extended analysis of each technology consisting of a brief introduction, technical specifications and special characteristics, network infrastructure and security considerations. Afterward, a theoretical comparison of these four technologies in terms of coverage, range, cost, bandwidth, energy efficiency, frequency bands, regulations, interference, capacity, mobility etc. is included. According to these findings, selection of the most suitable technology of Industrial IoT applications is proposed and discussed.

3. Practical implementation of the chosen technology into different topologies/cases that include urban/rural and indoor/outdoor scenarios. From these measurements, very useful parameters can be extracted such as the average value of the received signal strength indicator (RSSI) and signal to Noise Ratio (SNR) or the outage capacity which is the probability of the transmission to be in outage. After processing the data from this deployment, a comparison between practical and theoretical findings is presented.

1.5. Organization of Thesis

This Master thesis content is divided into six chapters. In the first chapter, Industrial IoT and Low Power Wide Area Network background is described. In addition, the problem definition and the method to solve are determined and previous academic work that consisted of the basis for this research is given credit.

The second chapter provides a theoretical analysis by describing in detail the core characteristics of the targeted LPWA technologies: Sigfox, LoRa, NB-IoT, and CAT-M1.

In the third chapter, a thorough comparison of the four technologies regarding technical aspects such as coverage, range, cost, bandwidth, energy efficiency, frequency bands, regulations, interference, capacity and mobility, is provided. Furthermore, based on this theoretical comparison, the choice of the most suitable solution and the reasons behind it are being presented and explained.

After the technology to be used, has been decided, the fourth chapter provides all the practical implementation content including equipment setup, measurement scenarios based on different topologies and the final processing of the measurements followed by result graphs on the performance of the system studied.

In the fifth chapter, conclusions about the suitability of the selected technology for Industrial IoT applications are extracted and discussed in further detail. In addition, theoretical and practical findings are compared in order to enable verification and ensure the reliability of the technology.

Finally, the sixth chapter discusses potential future work that needs to be pursued and provides suggestions on critical aspects that can be improved.

The Master thesis topic was provided by HMS Industrial Networks and was pursued in collaboration with the Department of Electrical and Information Technology (EIT) of Lund University. Ahmad was responsible for the theoretical analysis of LoRa and NB-IoT, comparison chapter, and of the field measurements in the area of Malmö. On the other hand, Nikolaos was responsible for the theoretical analysis of Sigfox and CAT-M1, field measurements in the area of Lund and conclusion section. The remaining work was equally distributed and pursued by both parties.

Chapter 2. Technologies

2.1. Sigfox

2.1.1. Introduction

Sigfox is a company that was created in 2010 and has its headquarters near Toulouse, in France. In collaboration with various network operators in each country as partners, it provides global wireless networks that aim to enable Low-Power Wide-Area solutions in the continuously evolving world of the Internet of Things [9]. It follows an approach similar to cellular network operators but differentiating in the sense of providing services to devices that are characterized by low-power consumption and consequently by low-cost performance [3]. Already being deployed in more than 45 countries, Sigfox' vision is to become a global leader in the sector of LPWA networks and IoT connectivity [9].

2.1.2. Technology

Ultra-Narrow Band

As far as the technology used is concerned, Sigfox utilizes part of the unlicensed Short-Range Devices (SRD860) and ISM frequency band (868 MHz in the European region and 915 MHz in the United States respectively) [9]. More specifically, in order to deliver each message, it utilizes 192 kHz of the SRD860 band based on the Ultra-Narrowband modulation technique. That means that every message requires only 100 Hz in order to be transmitted, leading to a data rate equal to 100 bps in the region of Europe as a consequence [1]. Due to UNB modulation, each message's power is concentrated within a very small bandwidth and that is the reason why Sigfox technology is resilient to interference and noise levels as depicted in Figure 2.1 [9].

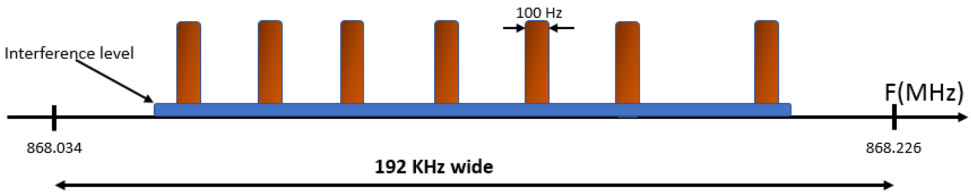

Figure 2.1. UNB Modulation Technique & Interference Resilience

For transmissions from the devices to the base stations (uplinks), Sigfox uses Differential Binary Phase-Shift Keying (DBPSK) modulation. For downlink transmissions (which are less frequent), Gaussian Frequency-Shift Keying (GFSK) technique is being used.

Duty Cycle & Sleep Mode

According to ETSI regulations regarding the usage of the publicly available Short-Range Devices (SRD860) frequency band just available in 1% of the time, 140 messages of length equal to maximum 12 bytes each, can be transmitted per day for uplink transmissions. Up to 12 bytes per message might not sound like a lot of data to demanding users, but in fact, it is proven to be more than enough for classic IoT cases. Such cases include asset tracking by sending the asset's GPS coordinates (equal to 6 bytes), monitoring of the climate changes by sending the temperature values (2 bytes) and so on [9].

On the other hand, for downlink transmissions, only 4 messages of length equal to maximum 8 bytes each, can be transmitted per day. Therefore, it can be noticed that the relation between uplink and downlink in Sigfox technology, is clearly asymmetric and therefore there cannot exist downlink acknowledgment for every single uplink message [1]. However, not using the channel 99% of the time, as shown in Figure 2.2 [9], means that the devices are in sleep mode and end up saving a lot of battery-life and eventually lead to important cost reduction.

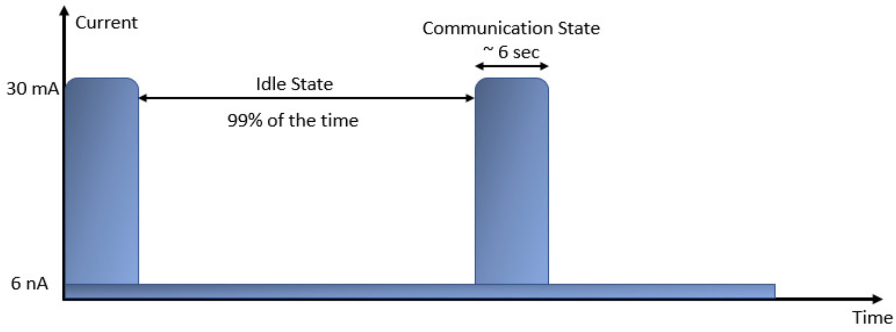

Figure 2.2. Active-Sleep Mode in Sigfox

Frequency & Time Diversity

In order to compensate for the lack of acknowledgments for each uplink message, Sigfox takes advantage of frequency and time diversity. The device transmits the same message 3 times using 3 different time slots, each having a different frequency, as shown in Figure 2.3 [9].

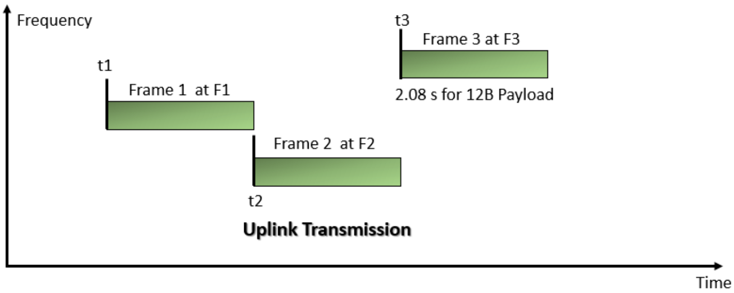

Figure 2.3. Frequency/Time Diversity in Sigfox

Spatial Diversity

Base stations that the device is within their range will receive the transmitted message ensuring that there is spatial diversity as well [9]. The spatial diversity is shown in Figure 2.4 [9].

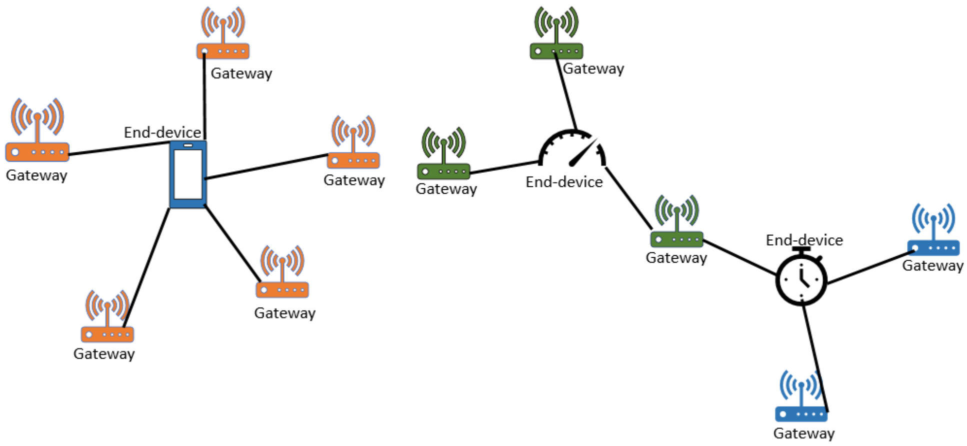

Figure 2.4. Spatial Diversity in Sigfox

2.1.3. Network Architecture

As discussed in the introduction of the technology, Sigfox not only partners with network operators in each country but also builds its own base stations in order to deploy its network around the globe. Because of the frequency band used, the propagation and coverage work pretty much similar to traditional cellular network systems.

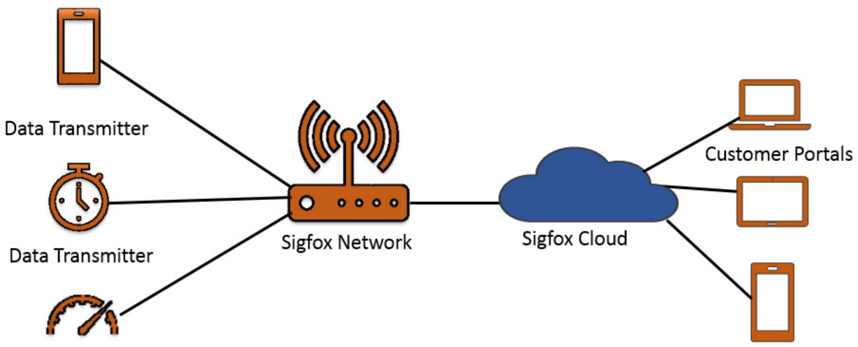

Figure 2.5. Sigfox Network Architecture

The deployed base stations have therefore a wide area of coverage and can be limited to just a few base-stations in order to satisfy the needs of a whole area (country or city). In Figure 2.5 [9], the principal network architecture of Sigfox is depicted. The network is forming a Star topology, data transmitters (usually sensors that perform smart metering applications, etc.) connect to the Sigfox base stations using the air as a medium, just like radio frequency waves. Once the messages are received by the base stations, then they are redirected to the Sigfox cloud network using the existing 3G/4G or Ethernet backhaul by mobile network providers.

As a final stage, they are directly depicted on the Sigfox backend server or directly at the customer's portal applications. The customers are able to create callbacks or further applications in order to exploit the messages' content in the way they need to [11].

2.1.4. Security

Security is one of the most important issues that the IoT industry has to face. Data alongside its transmission must have a certain characteristic such as integrity, confidentiality, and authentication in order to avoid any unfortunate and harmful scenarios.

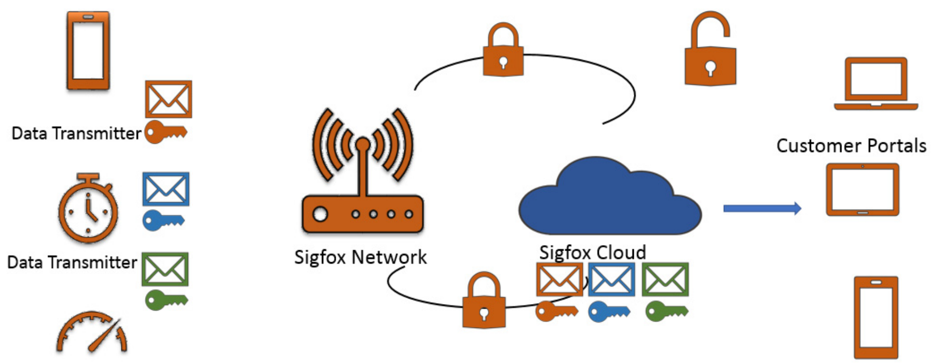

Figure 2.6. Security in Sigfox

Sigfox implements several layers of security starting from the device itself and ending to the application on the web server, depicted in Figure 2.6 [9]. In order to initiate the transmission and communication with the Sigfox cloud, each message must have a unique authentication key which is secret. Then the devices transmit their encrypted messages to the base stations using this secret key and create a unique signature for every single message. In order to avoid redundancy of the same message, a sequence number is added to the radio packet frame.

Moreover, as far as the radio transmission side is concerned, the fact that each device sends three messages in different times and frequencies, adds an additional layer of security since the choice of the receiving base stations is not fixed in advance. In addition, the deployment of UNB modulation in combination with space diversity (three base stations receiving the same message) reassures the integrity of the data, preventing any loss due to interference or jamming from other sources.

Regarding the transmission from the base stations to the Sigfox cloud, the connection is being established using a secure and encrypted Virtual Private Network (VPN). On top of that, Sigfox cloud is virtualized and replicated on various private data centers on different locations.

Finally, the customers connect to the backend servers (cloud) to exploit their data via APIs or callbacks, using the robust HTTP protocol. It is worth to be noted that while a device is in sleep mode, it becomes immune to any form of communication from possible hackers or eavesdroppers, which makes it work like a built-in Firewall system [9].

2.2 LoRaWAN

2.2.1. Introduction

LoRaWAN standard is innovated by Semtech, first released in 2015 and developed by LoRa Alliance as a wireless communication standard operating within the unlicensed bands. The name stands for Long Range Wide Area Network.

It is important to distinguish between LoRaWAN and LoRa because they are not interchangeable terms. LoRa defines the modulation in the physical layer, whereas LoRaWAN is a definition of MAC protocol that supports low power, long range and high capacity in LPWA networks. In general, communication standard and system architecture determine the overall technical performance of the technology, such as energy efficiency to save battery charge of the end-devices, the capacity of the network and dedicated data rates for different applications which can be supported by the network. This technology's physical layer and MAC layer are shown in Figure 2.7 [12].

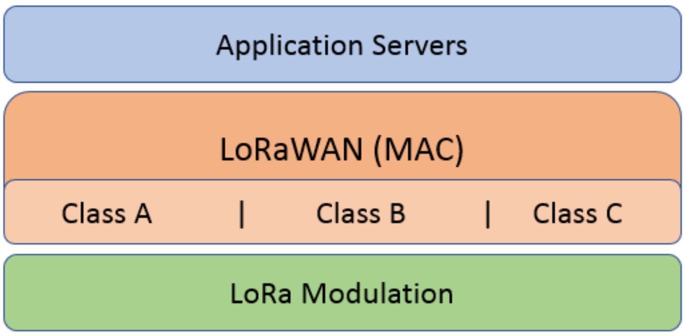

Figure 2.7. LoRa and LoRaWAN Layers

2.2.2. Technology

Coverage and Link Budget

The key feature in LoRaWAN standard is LoRa which is a part of the physical layer and describes the modulation that maintains the long-range ability in LoRaWAN.

LoRa is based on chirp spread spectrum (CSS) technique. Compared with modulation schemes utilized by other wireless systems such as Frequency Shift Keying (FSK), LoRa holds the same low level of power consumption and achieves longer range communication. As a modulation technique, chirp spread spectrum affords important features such as very long ranges similar to the ones offered by narrow-band networks, high robustness against interference and propagation losses [13]. The benefit of using Lora is that a whole city or region can be covered by deploying only one gateway [12].

That was proven during a research made by Aalborg University in collaboration with Telenor's commercial cellular network, to test the coverage of different technologies including LoRaWAN in 7800 km^2 of rural and urban areas. The base stations were supported with 10 dBi omnidirectional antennas and the used transmitted power was 14 dBm which is the maximum value allowed by LoRa. Channel modeling depends on the environment which influences the signal propagation by means of large-scale fading, small-scale fading, and path loss. The used propagation model was 3GPP macro non-line-of-sight model. The result shows that LoRa provides full coverage in outdoor environment up to 11 km with low coupling loss equal to 144 dB. The maximum coupling loss achieved was 155.5 dB with 24% outage capacity for deep indoor environment [6].

The suitability of LoRa for industrial purposes regarding coverage is reasonable given the fact that an area of 5 km radius could easily be covered to connect hundreds of end-devices (large -scale capacity) with low cost.

Power consumption

End-device transmits uplink packets to the gateways in a similar way to Aloha protocol, i.e. devices transmit when data is ready to be sent whether this transmission is scheduled or action-based using medium access mechanism that has small bandwidth utilization. Furthermore, there is no synchronization between end-devices and gateways. This asynchronization saves power considerably if it is compared to other technologies (i.e. cellular systems) where mobile-devices regularly wake up to update the network about its situation (base station, routing area or location area) and scan for messages that the devices can be reached for downlink transmission. LoRa solves this by only allowing downlink transmission after uplink transmission as it is specified in three classes which will be explained henceforth. The avoidance of downlink transmission as much as possible and using such medium access mechanism increase battery lifetime which can last for ten years in LoRaWAN. According to a lab experiment where data was transmitted repeatedly in a long-range scenario, the lifetime of 2000 mAmph (5.1 Wh) battery was estimated to reach 32 years [14]. As far as power efficiency is concerned, LoRaWAN enables three kinds of End-devices which differentiate in downlink transmission schedule to obtain more saving in power, in cost of latency though.

Class-A

End-devices of class-A shown in Figure 2.8 [12], have two slots for downlink transmission after one uplink transmission, therefore end-devices consume the lowest power for their operations compared to other classes. Uplink transmission window is dedicated by end-device according to its need in a similar way to Aloha protocol. [15]

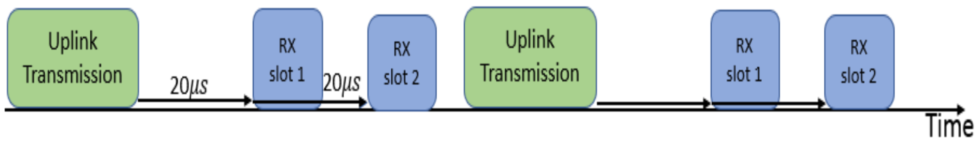

Figure 2.8. Class-A End-Devices

Class-B

In this class shown in Figure 2.9 [12], a modification is made in terms of receiving slots. One more downlink transmission window (ping slot) can be dedicated by the gateway according to its need in a predefined time and synchronized using Beacon frames. [15]

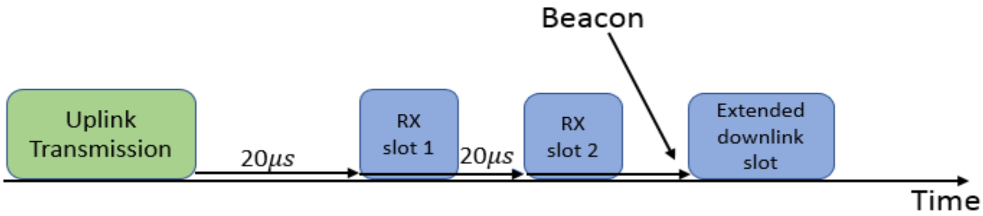

Figure 2.9. Class-B End-Devices

Class-C

Class-C end-devices shown in Figure 2.10 [12] allow constantly downlink transmission after uplink transmission. End-devices consume more power but provide less latency in the system. This class is suitable for applications that require more downlink transmission [15].

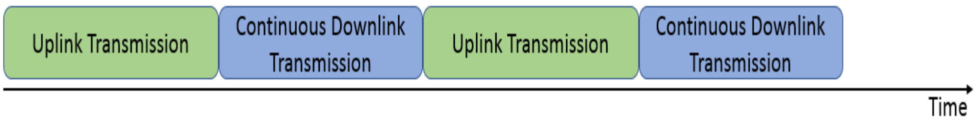

Figure 2.10. Class-C End-Devices

All classes offer bi-directional transmission. But it is not necessary that packets are acknowledged. In the case of Class-A end-devices, acknowledgments should be sent during the first or the second reception slot otherwise acknowledgments will never be received. End-devices transmit packets when they are ready. Moreover, LoRaWAN has confirmed or unconfirmed types of messages [15].

Class-A is available by default on all end-devices. The design of these classes has a significant influence on battery life. End-devices will only wake up for strictly predefined time slots when they have data to send, which saves energy compared to the frequent need for synchronization in cellular systems [15].

It can be noticed at this point that LoRaWAN allows variant options that are suitable for different applications. This feature gives a trade-off between energy consumption and latency where the system has low latency in cost of more power consumption and vice versa [15].

Radio spectrum

Different frequency bands are used for LoRaWAN in US and Europa within unlicensed bands. In the US, LoRaWAN operates within the industrial, scientific and medical (ISM) band 902-928 MHz, in Europa, it operates within ISM band 443 MHz, and Short-Range Device (SRD860) band 868 MHz. LoRaWAN offers scalable bandwidths of 125, 250, 500 kHz. Short Range Device (SRD860) band is unlicensed and can be used by anyone without paying a cent, but the usage of the SRD860 band is regulated by the regional government that puts limitations on the frequency and transmitted power. European regulations, approved in 2017, put a limitation on the transmitted power to be between 25-100 mW, and limitation on frequency as a duty cycle to be 1% of the channel as a maximum value in each sub-band [16].

Duty Cycle is defined as the part of time where the source is available for transmission. The SRD860 band is divided into sub-bands in order to exploit bands as efficiently as possible according to regulations on duty cycle. When an end-device sends on one sub-band, this sub-band cannot be re-used for a specific amount of time depending on limitations on duty cycle. This waiting time can be calculated as follows on (1) [16]:

$$\text{Waiting time} = (\text{time on air}/\text{duty cycle}) - \text{time on air} \qquad (1)$$

Time on air is the time needed to send an uplink transmission. For example, for a device which takes 0.4 sec to send data over a predetermined channel, the channel will not be available to use for 399.6 sec. However, if more than one sub-channel is available for a device, the aggregated duty cycle is calculated by summing duty cycles of all sub-bands [16].

The whole system (end-device/gateways) operates with respect to this limitation. But some strategies can be followed by the operator to utilize resources efficiently such as sending a small amount of data which needs less time on air, communicate with a less busy gateway and sub-channel.

Adaptive Data Rate

LoRaWAN permits end-devices to use one of the dedicated data rates which are known as adaptive data rates. That can be done in cooperation between the end-devices and gateway under the condition of almost static end-devices because the changes in the radio channel should be too slow. Adaptive data rate means that the network is able to optimize and reduce the power consumption and utilize the spectrum efficiently by using no more than the bandwidth that is needed to send data. However, this feature qualifies the network to have a very high capacity. This is suitable for industrial networks because of the direct effect on battery lifetime of the nodes and network capacity.

Adaptive data rates can be performed by either end-nodes or gateways through MAC commands. From this aspect, there are three factors that play an important role to obtain the right decision: transmission power, spreading factor and bandwidth. Therefore, the modulation scheme used for LoRa (chirp spread spectrum) has an essential significance [15].

Bandwidth

LoRaWAN allocates sub-bands with a bandwidth of 500 kHz, 250 kHz and 125 kHz. Depending on the regional limitation, only 250 kHz and 125 kHz are used in Europe [16].

Spreading Factor

Spreading factor is defined as the ratio of the chip rate to the pulse rate, where the pulse is represented by multichip.

LoRa uses spreading factor between 7 and 12. SF7 is the fastest as it takes less time on air and SF12 is the slowest with the longest time on air. Consequently, the higher the distance, the higher SF is.

The relationship between the three factors is considered in (2) and some distinguished data rates indicated from 0 to 6 are shown in Table 2.1. For example, using 125 kHz bandwidth with SF7 gives double data rate than the same bandwidth with SF8.

In other words, by reducing the spreading factor by 1, double data rate can be sent in the same bandwidth at the same time. By reducing the spreading factor, it will become harder for the base station (Gateway) to receive data packets properly. This leads to the fact that the spreading factor is also related to the distance between the end-nodes and the gateway. A lower spreading factor can be efficiently used as the distance is shorter [16].

$$\text{Data Rate} = \text{SF} \cdot \text{BW} / 2^{SF} \qquad (2)$$

Data Rate	Configurations	Physical bit rate (bps)	Payload size (Bytes)
0	LoRa, SF12,125kHz	250	51
1	LoRa, SF11,125kHz	440	51
2	LoRa, SF10,125kHz	980	51
3	LoRa, SF9, 125kHz	1760	115
4	LoRa, SF8, 125kHz	3125	242
5	LoRa, SF7, 125kHz	5470	242
6	LoRa, SF12,250kHz	11000	242

Table 2.1. LoRaWAN Adaptive Data-Rate

2.2.3. Network architecture

LoRaWAN network is described as long-range star architecture. In contrast to mesh architecture where data is transmitted from node to node to reach the destination in long range and large cell size, LoRaWAN architecture increases network capacity, reduces complexity and consequently increases the power efficiency of nodes by eliminating extra data forwarding between nodes.

LoRaWAN networks consist of the following components:

1. End-devices that are peripherals of the LoRaWAN network such as sensors or control tools. End-devices connect usually to more than one gateway actively and send same data to them simultaneously.
2. Gateways that are connected with end-devices and with servers via either cellular, Ethernet or Wi-Fi connections.

3. Servers that are cloud-based managed within the network where all operations are performed i.e. removal of duplicated data packets, implementation of security control, transmission of acknowledgments if needed through the nearest gateway and deployment of adaptive data rate, etc. [12].
4. Applications server that controls the function of end-devices and collects information from them such as humidity information if humidity sensors are being used for example.

As shown in Figure 2.11 [12] end-devices send data to multiple gateways, using LoRa protocol, which in turn forward to the cloud-based server via either Ethernet or cellular backhaul. The user gets the information about its end-device from the server using applications designed for this purpose. [12]

Such networks are fully compliant to industrial networks. Industrial networks have most likely designed a cloud-based server for their applications such as gas tanks monitoring, temperature and humidity metering. As a consequence, LoRaWAN networks prove to be suitable for industrial purposes because there is no need to make frequency planning due to using unlicensed frequency band. That offers flexibility in designing a system that fulfills specific requirements in the industry. LoRaWAN supports mobility through an association between end-devices and cooperative reception.

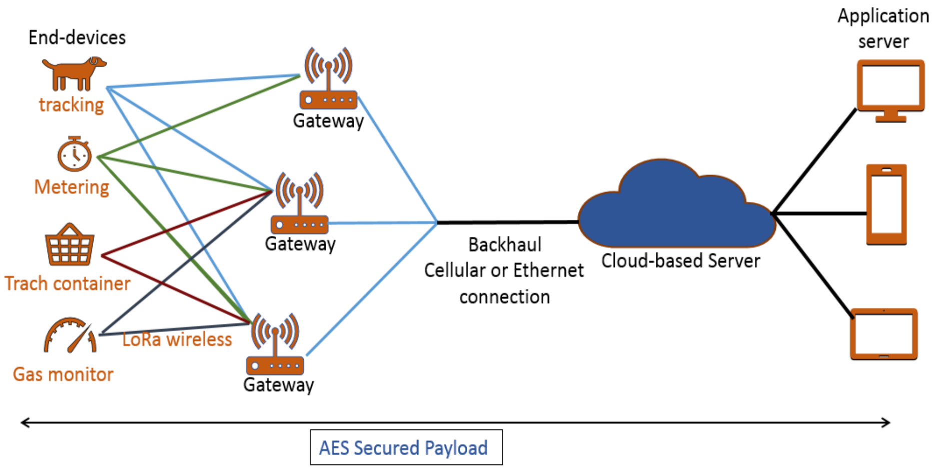

Figure 2.11. LoRaWAN Network Architecture

2.2.4. Security

LoRaWAN uses different authentication keys during connection process between end-devices and gateways, Gateways and server. All keys have a length equal to 128 bits and are encrypted using Advanced Encryption Standard (AES). The keys are described as follow:

1. Serving Network Session Integrity Key (SNwkSIntKey) is an end-device key utilized to verify Message Integrity Code (MIC) of half uplink data and all downlink data [30].
2. Network Encryption Session Key (NwkSEncKey) is a specific key for end-device to decrypt and encrypt MAC commands in uplink and downlink transmission [30].
3. Application Session Key (AppSKey) is an end-device key that is used by applications server and end-device in order to encrypt and decrypt data between them. This data is a point to point encrypted which means that data is protected in one hop between end-device and application server. In case a third part interferes and changes the data in transit, a reaction on the application server will be created which will be taken into consideration by the network server to prevent it from being forwarded [30].

These keys are singular for each session and each end-device and are generated when end-devices are activated. Depending on the type of device activation, the keys should be generated and stored in a specific way to be protected from malicious parties. LoRa is also part of the security procedure because the Chirp Spread Spectrum technique is robust against noise interference and it is also robust against malicious users. This method is used in the most critical case to protect the content of data for military communication, which makes this standard more attractive for industrial LPWA networks [15] [30].

2.3. Narrow-Band IoT

2.3.1. Introduction

Third Generation Partnership Project 3GPP completed in 2015 the formation of a working group to integrate Huawei's cellular Internet of Things technology (NB-CIoT), which is standardized with a partnership of Cambridge-based Neul and Vodafone, and LTE technology introduced by Nokia, Ericsson, and Intel. The resulted standard is Narrow Band-IoT. The first NB-IoT standard was completed in June 2017 and has been included in 3GPP Release 13 [17].

3GPP determined five targets in Release 13 (R13) for Machine Type Communication MTC (This term is used by 3GPP to indicate to Machine to Machine communication). The targets were to improve indoor coverage in high loss locations, to enable continuously the increasing number of IoT devices, to lower the cost of process procedure and units, to enable less power consumption and to support latency features [7].

The support of the world's most important telecommunication companies, the fact that the existing wireless networks can deploy the technology and the fact that the technology can be operated in an authorized frequency band, are the three factors that ensure a solid and stable industrial deployment for this technology [7].

NB-IoT particularly aims to serve low throughput IoT applications. It is designed to have better coverage and minor cost than other IoT cellular technologies. However, NB-IoT supports the connection of million MTC devices and applications. This connection is characterized by low throughput, infrequent data transmission [7].

A strategy of two levels is adopted by 3GPP to handle different challenges imparted with MTC services. The first level is the transition strategy that targets to reuse and upgrade the existing network in order to support IoT applications. The second level is a continuing long-term strategy that will come up with a new wireless radio technology NB-IoT which will enable the increasing demand for IoT services and devices [7].

2.3.2. Technology

High power efficiency

In IoT technology, it is required that battery lifetime should last at least ten years for low data rates and sub 1GHz frequency. This requirement is fulfilled in NB-IoT by two technologies, including Power Saving Mode PSM and expanded Discontinued Reception (eDRX). In PSM, the NB-IoT device is still registered but are not available for downlink transmission in order to send more information. eDRX is a new technology that allows extended sleep durations and decreases unnecessary wake-up for receiving downlink transmission. Figure 2.12 [7] shows eDRX, PSM and availability of end-nodes to scan for synchronization [7].

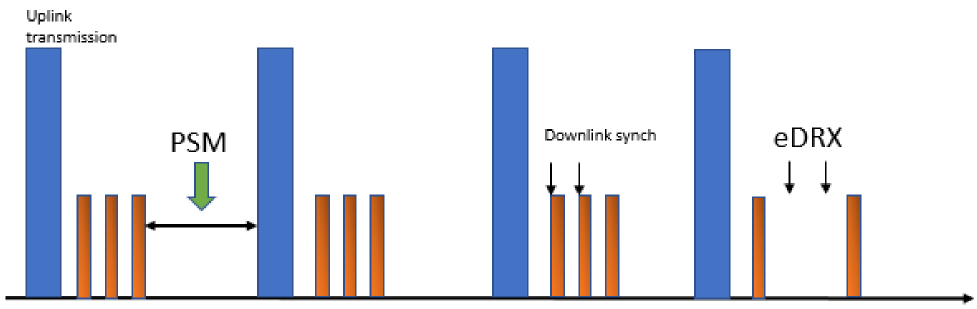

Figure 2.12. Power Saving methods in NB-IoT

There is a relation between battery lifetime and coupling loss experienced by end-devices until the data reaches the base station. The coupling loss increases significantly power consumption. It is estimated that a 5-Wh battery can last for 11 years transmitting 25 bytes per hour in a 154dB coupling loss environment. From an industrial deployment point of view, this result of power consumption is totally approved for the majority industrial applications. Different values of battery lifetime under different circumstances of radio channel loss and data rates are shown in Table 2.2 [7].

	Battery life (year) in coupling loss (dB) configuration		
Message size	144 dB	154 dB	164 dB
50 bytes/ 2 hours	22.4	11	2.5
200 bytes/ 2 hours	18.2	5.9	1.5
50 bytes /day	36	31.6	17.5
200 bytes /day	34.9	26.2	12.8

Table 2.2. Battery Lifetime in Different Configurations

Coverage and Latency Sensitivity

In a study made by Aalborg University in Denmark [6], a commercial cellular network that composed of 2G, 3G, and 4G deployments, was used. The study was deployed in 7800 $km^2$of urban and rural areas. The total area consisted of 319 sites provided with sectorized antennas with beam radiation of 65 degrees of average gain 17 dB. This study considered the transmitted power to be equal to 23 dBm in uplink transmission, and 43 dBm in downlink transmission following the standard in 3GPP. 3GPP Rural Macro Non-Line of Sight model was used as the channel model in rural scenarios, and 3GPP Urban Macro Non-Line of Sight model was used in Urban scenario. Results related to NB-IoT show that the technology achieved less than 1% outage capacity in outdoor coverage, i.e. more than 99% of data was successfully delivered. For Indoor of 20 dB breakthrough loss urban area, end-devices achieved about 1% outage capacity due to a maximum link loss of 164 dB which is significantly better than other unlicensed technologies. This result has been confirmed by simulated data of TR45.820 which provides coverage for 164 dB coupling loss for a test presented in guard-band and in-band deployment. NB-IoT may encounter considerable interference because of using LTE system’s existing networks. However, this issue can be solved by upgrading the core network of NB-IoT for long-term improvement [6].

In a scenario with less than 1% outage capacity and full coverage, latency increases because of fast retransmission of missing data. However, simulated data of TR45.820 shows that latency is between 6 and 10 secs of full coverage for maximum coupling loss. As a consequence, coverage and latency are inversely related in NB-IoT [7].

Compared to coverage of GSM, NB-IoT has 4 times larger radius coverage than in GSM in which maximum link loss is 144 dB for a device's transmitted power 33 dBm. As mentioned before the main goal when designing NB-IoT, is to achieve an enhancement in coverage of 20 dB at least over cellular standard. Increasing the maximal retransmission times in downlink and narrowing the bandwidth enhance the coverage of NB-IoT although uplink transmitted power is 10 dB less than in GSM (only 23 dBm in NB-IoT) [7].

Spectrum Resources and Technical Features

Internet of Things will be the most attractive communication service for a large number of users. therefore, the development of NB-IoT will be supported by the owners of the spectrum, worldwide.

The bandwidth of NB-IoT technology is 200 kHz. Different modulation schemes are deployed in downlink and uplink to acquire better usage of the licensed spectrum. Table 2.3 [7] shows the different technical features of NB-IoT. NB-IoT implements QFSK modulation and OFDMA as Multiple Access scheme with sub-carrier spacing 15 kHz in downlink transmission. On the other hand, in uplink transmission, BPSK or QPSK is utilized with SC-FDMA with tune spacing 3.75 kHZ and 15 kHz or Multiple carrier FDMA with 15 kHz as aggregation access technique. It is clearly figured out that a modification of LTE is needed to support the unique requirements of NB-IoT which use the existing structure and technical draw of LTE [7].

Physical Layer	Technical Characteristics	
Uplink Transmission	QPSK modulation	
	SC-FDMA	Interval 3.75 =>DR 160 kbps
		Interval 15 kHz => DR 200 kbps
	Multi-Carrier FDMA	
Downlink Transmission	QPSK Modulation	
	OFDMA subcarrier space 15 kHz => data rate 160- 250 kbps	

Table 2.3. Physical Layer in NB-IoT

Sub-carrier spacing of 3.75 provides 48 sub-channels, accordingly, 12 sub-channels are provided with 15 kHz subcarrier spacing in SC-OFDM calculated using (2).

$$W_{ofdm} = \mathrm{k} \cdot \Delta f \qquad (2)$$

where W_{ofdm} bandwidth, k is the number of sub-channels and Δf is sub-carrier spacing.

The range covered by 3.75 kHz subcarrier spacing is higher than the later one due to higher density. But the complexity of extracting information is significantly higher and consequently, the cost of end-devices is higher. NB-IoT provides data rates in uplink and downlink transmission of 67 kbps and 30 kbps respectively as maximum values. [7]

Currently, NB-IoT works under the condition of 3GPP specification which provides only Frequency Division Duplex with a bandwidth of 180 kHz for three deployment scenarios (shown in Figure 2.13) [7]:

1. Stand-alone mode: NB-IoT uses a frequency band outside the bands used by LTE
2. Guard band mode: the frequency on the edge of LTE is utilized

3. In-band mode: one resource block is used in the frequency band of LTE.

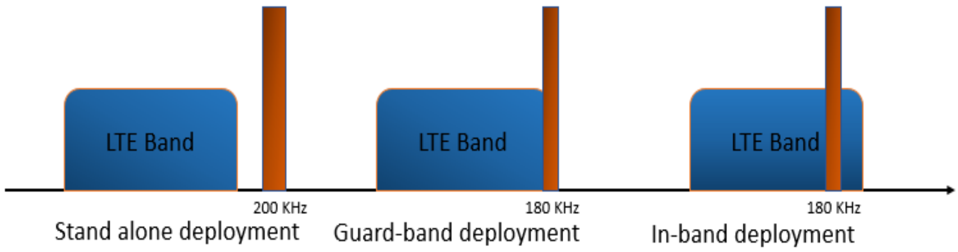

Figure 2.13. Deployment Modes in NB-IoT

Important technical features for future development

1. Mobility: in the latest specification of 3GPP Release 13 NB-IoT was designed to support static end-nodes. In R14 handover between cells in connected state will be supported. End-nodes measurement reporting will also be supported because it is required to enable switchover.
2. Multi-cast: Downlink transmission is supported in NB-IoT with a feature of fast retransmission from a base station to end-nodes, but R13 doesn't provide sending the same message to a large number of end-nodes which could waste the system bandwidth. Multi-cast could be supported in R13 as a typical possibility in IoT.
3. Localization: Some features like Positioning Reference Signal (PRS) and Sounding Reference Signal (SRS) are disabled in NB-IoT in order to save power which result in the inability to localize end-nodes accurately. New features can be added in future to handle with localization issues [7].

2.3.3. Network Architecture

Five main parts form the Network design of NB-IoT, including:

1. NB-IoT end-devices: Most IoT devices, used for industrial purposes, are provided with access to NB-IoT network if they have a proper SIM card from NB-IoT telecom service providers.

2. NB-IoT Base station: The base station which is owned by telecom service provider and supports all deployments modes. This can also be called evolved Base station eNodeB or eNB
3. NB-IoT core network: The bridge connection between base stations and NB-IoT cloud. NB-IoT core network is a legacy of Evolved Packet System (EPS) used by LTE, which is modified to suit NB-IoT deployments. These modifications include two optimizations for the Cellular Internet of things (CIoT).

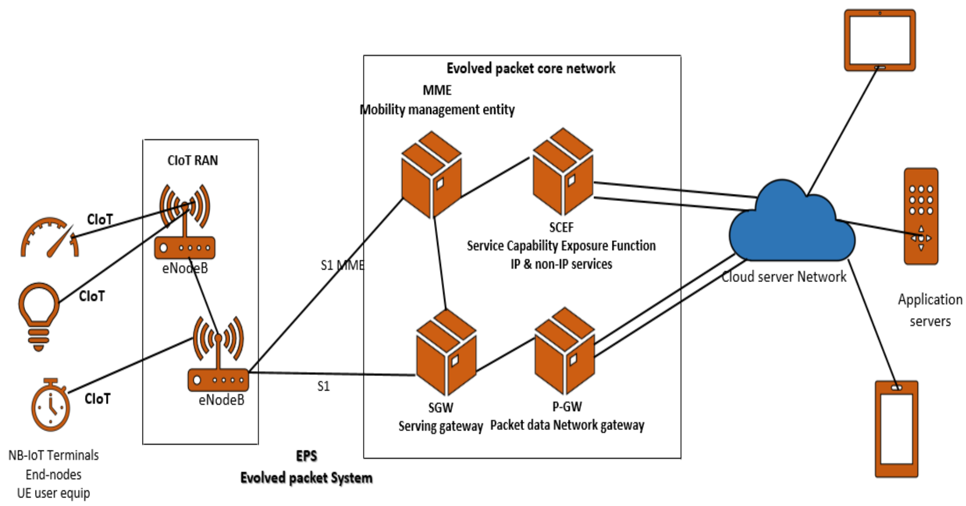

Figure 2.14. NB-IoT Network architecture

Control Plane CIoT optimization

The path of transmitting data from end-devices to the cloud goes through eNB to Mobility Management Entity (MME) of LTE and then is being transferred either via Serving Gateway (SGW) to Packet Data Network Gateway (PGW), or through Service Capability Exposure Function (SCEF) which is a new node specifically designed for MTC to deliver non-IP data in the control plane. NB-IoT cloud-based server is directly connected to them as shown in Figure 2.14 [8]. The result of this optimization is that data is sent on the signaling bearer instead of setting up the radio bearer before which enables infrequent transmission and smaller data packets [7] [8].

User plane CIoT optimization

Data packets take the same path in User Plane Optimization as the traditional data traffic via SGW and PGW without crossing through new node SCEF to reach the cloud-based server. This may add some additional data on the connection, but it simplifies the transmitting of data sequences [8].

4. NB-IoT cloud-based server: The cloud platform that processes all different types of data and applications, instead of doing that in end-devices to save power and extract complexity from the end-nodes.
5. Applications that are used by the end-user to collect the data from nodes or sensors about a specific purpose [7].

The fact that the network architecture of NB-IoT is designed based on the LTE network with a particular modification to enable NB-IoT services could be an advantage for using NB-IoT technology in future smart cities and industrial IoT applications because of its guaranteed QoS and high data rates support.

2.3.4. Security

All IoT technologies share basically similar requirements for security. NB-IoT has some differences related to Low Power feature. Peripherals in conventional IoT technologies contain complicated transmission protocol and strong security plan which demand high power consumption and frequent battery charging. However, NB-IoT end-nodes are low-power devices that is not designed to handle complex and high-energy security issues. Consequently, any simple security vulnerability can lead to larger security problem especially in such large-scale networks like NB-IoT supported with lightweight security systems [7]. NB-IoT supports security requirements (shown in Figure 2.15 [8]) through IoT architecture which consists of three layers.

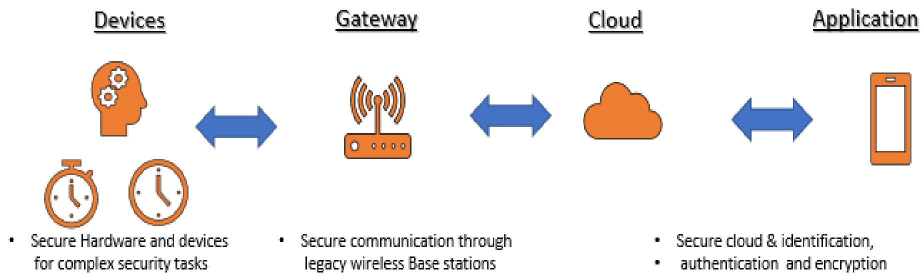

Figure 2.15. NB-IoT Network Security

Perception Layer

The perception layer is corresponding to the physical layer and Data link layer in the OSI model and is considered to be the basis for higher layers and services. However, this layer includes end-nodes like metering devices, temperature sensors etc.

A comparison between conventional IoT and NB-IoT security systems is introduced to better understand the requirements that are implemented by NB-IoT. In this layer, encryption of data, integrity verification and authentication of identity are implemented in IoT for protection. These algorithms include random and deterministic key approaches and password security. In NB-IoT a light password is utilized for safety because of low power restrictions. End-nodes in NB-IoT are directly connected to the base station in the cell which prevents problems sourcing from routing security [7].

Transmission Layer

NB-IoT deploys a network for a large area or a whole city. Therefore, not only many security problems can be avoided but also maintenance and easier management can be achieved compared to conventional IoT network.

A massive number of end-nodes can be served by one NB-IoT network. This leads to a great challenge regarding how to perform identity authentication in real time for up to hundreds of thousands connections efficiently. Another challenge is how to protect the wireless network from interference signals that can be transmitted by hackers to affect the network performance. IoT applied a key-agreement mechanism and an end-to-end authentication mechanism as security standards, but an optimized implementation of these mechanisms is still under construction for NB-IoT [7].

Application Layer

The application layer is the last station for data. At this layer, data is stored, analyzed, processed and managed sufficiently. A much larger amount of data is received at the application layer coming from perception and transmission layers of NB-IoT than in conventional IoT systems due to large-scale. NB-IoT performs efficient data integrity verification and synchronization methods. Many mechanisms are used to deal with different problems related to massive heterogeneous data, including mechanism to delete the duplicated data, mechanism to deconstruct from the node itself [7].

2.4. CAT-M1

2.4.1. Introduction

CAT-M1 or else known as LTE-MTC (Long Term Evolution- Machine Type Communication) or just LTE-M for simplification, is one of the two proposals of 3GPP for cellular Low Power Wide Area applications and was launched to the market in 2016. However, continuous improvements are being carried on and the last launch of the technology is expected to take place in June 2018 [18].

The main idea is that the CAT-M1 IoT devices are connected wirelessly directly to the existing LTE network (4G). As a consequence, there is no need for the deployment of new base stations or additional network infrastructure in general. Obviously, this sounds very attractive to the current network and mobile providers of LTE, since the transition to CAT-M1 is very direct and cost-effective [17]. LTE-M could be used efficiently for applications such as Smart Metering and Asset Tracking, as long as the coverage of the devices is supported by the LTE network.

2.4.2. Technology

As far as CAT-M1 technology is concerned, the solution has been tailored to the existing LTE technology for mobile applications. Specific chipsets are designed so that CAT-M1 uses only 1.4 MHz of the LTE band and operates half-duplex. These chipsets connected to an antenna unit each, form the CAT-M1 User Equipment (UE) [18]. The interesting part is that CAT-M1 can operate within any LTE bandwidth subset. Therefore, cost reduction is being achieved easily [19].

For the uplink, Single Carrier-Frequency Division Multiple Access (SC-FDMA) medium access scheme is being utilized with 15 kHz tone spacing and turbo code. The modulation technique is 16QAM. For the downlink, OFDMA is being utilized with 15 kHz tone spacing and turbo code. Again, the modulation technique is 16QAM. 3GPP specifications show that CAT-M1 devices on batteries can last for 10 years and that coverage can be extended to 156 dB of Maximum Coupling Loss (MCL) [19]. Data rates can be modified regarding coverage.

Power Saving Mode (PSM)

However, what makes CAT-M1 more interesting, is the addition of two performance modes of the chipset, that lead towards energy saving and power efficiency. One of them is the LTE Power Saving Mode (PSM), where the CAT-M1 UE is going to sleep mode most of the time and wakes up only for a very specific time slot in order to transmit data to the network as shown in Figure 2.16 [18]. After sending the data, it remains active in receiving mode for four specific time slots, just in case there is need to be reached by the network [19]. Therefore, each device being “sleep” most of the time, contributes greatly to the reduction of power consumption.

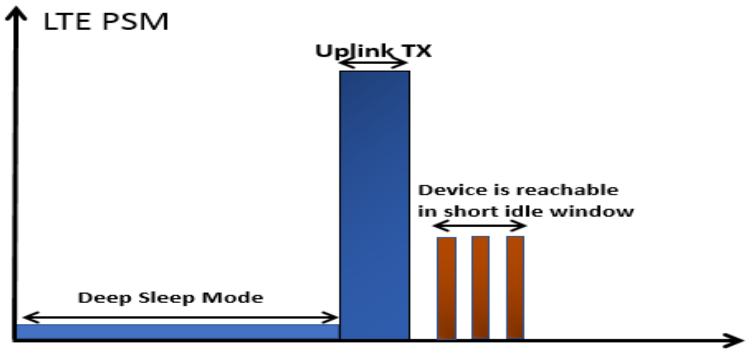

Figure 2.16. LTE Power Sleeping Mode (PSM)

Extended Discontinuous Reception Mode (eDRX)

The second mode is the LTE Extended Discontinuous Reception (eDRX) mode (Figure 2.17 [19]), where extended windows of sleep are added between LTE paging cycles which can be ranged from 10.24s to 44 min [19]. This mode is a very good alternative for CAT-M1 UE that are needed to stay always active and waiting for network feedback. Obviously, this mode is less power saving than LTE PSM due to the addition of more time slots whereas the device is “on”.

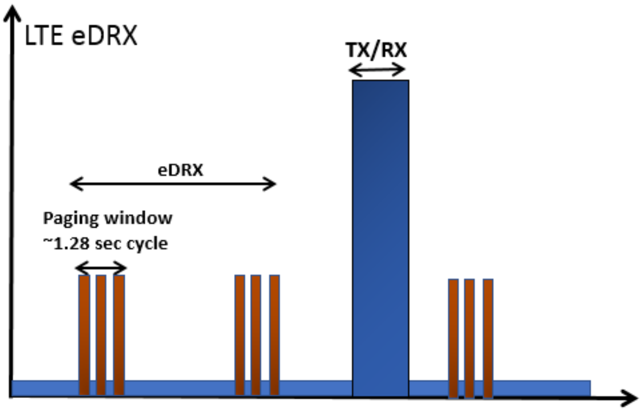

Figure 2.17. LTE eDRX Mode

2.4.3. Network Architecture

CAT-M1 is an attractive LPWA technology since it utilizes the existing LTE network architecture. The only additions that have to be made are the CAT-M1 UE implementation on the user side and just a software upgrade on the eNodeB base stations of the LTE network [20].

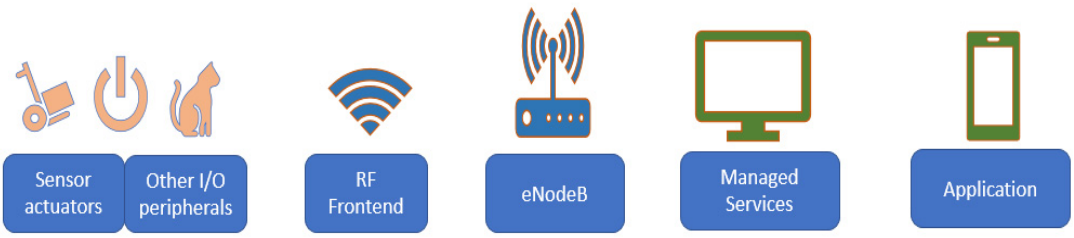

Figure 2.18. CAT-M1 Network Architecture

The User Equipment (UE) implementation involves the integration of a chipset and an antenna to the desired sensors. A SIM card is required as well to enable transmission and authentication through the network. As shown in Figure 2.18 [19], this unit connects directly to the LTE network without having the need to connect to any other gateways like in Sigfox or LoRaWAN. The LTE network consists of the Evolved Universal Terrestrial Radio Access (E-UTRAN) and Enhanced Packet Core entities. The eNodeB is responsible for the allocation of resources to the UE for both uplink and downlink transmissions and are also in charge of the state transition from idle to active(connected) mode of the UE. The existence of the Managed Services core network enables a secure and protected monitoring environment for all the data that is received. In the user's side, data and applications can be retrieved from the application server provided by the network operator of the region [21].

2.4.4. Security

Due to the fact that CAT-M1 technology is an integrated part of the existing LTE/3G infrastructure, it follows the same principles and methods to ensure secure and reliable end-to-end communication between end-devices and backend servers. However, because of the low-cost and less complex chipset modules provided for the end-devices, many security flaws and breaches arise. The need for the modules to endure for a long amount of the time, has made them more prone to malicious attacks or eavesdroppers. As a customer, physical security of the modules must be added as a security measure in order to prevent any malicious nodes or undesired interference. The remaining security procedure is mostly operated by the network providers according to 3GPP standards [21].

This security procedure includes mutual authentication between the UE and the LTE network which is conducted by the Mobility Management Entity (MME), included in the E-Packet Core network. Packets are encrypted and supported by integrity protective algorithms. Moreover, similar to GSM technology, the Authorization Centre (AuC) is responsible for the construction of security information based on security keys. This procedure ensures that eavesdropping is dropped, and messages are correctly distributed along the network [21] [27].

Chapter 3. Theoretical Comparison

3.1 Introduction

The aim of this section is to compare the performance of the four LPWAN technologies to conclude at the end with the most promising technology for deployment in industrial LPWA networks. The aspects considered in the comparison include power consumption, latency, suitability for real-time applications, quality of service, cost, mobility, security, availability, coverage, data rates and bandwidth.

3.2. Frequency bands and data rate

NB-IoT and CAT-M1 operate in licensed bands, while Sigfox and LoRaWAN use the unlicensed frequency band. Both frequency bands are sub 1GHz bands to get the advantage of long-range communication and smooth propagation characteristics. Some NB-IoT and CAT-M1 devices support higher bands of 1.7 and 2.1 GHz which is dedicated for some regions and carriers. Using the unlicensed frequency band is cost-free but works under regional restrictions which determine duty cycle and maximum transmitted power. That affects the latency and downlink transmission of Sigfox and LoRaWAN since each end-device can transmit uplink with 1% duty cycle. In downlink transmission the duty cycle is calculated per device considering thousands of devices which are connected to one gateway. CAT-M1's bandwidth of 1.4 MHz can be used in in-band wireless spectrum, allowing a highest data rate of almost 1 Mbps. Consequently, many additional features are allowed by CAT-M1 such as voice and mobility enhancement. NB-IoT uses a narrow band of 200 kHz in stand-alone deployment and 180 kHz in-band and guard band deployment, the bandwidth makes NB-IoT fit into existing LTE and GSM cellular networks, as 180 kHz is the size of one resource block in LTE and bandwidth of GSM is also 180 kHz. this bandwidth allows smaller data rates than CAT-M1 as shown in Table 3.1. Sigfox, on the other hand, allows the lowest data rate of 100-600 bps and with a maximum payload of 12 bytes/message which is considered to be the main drawback of Sigfox and limits its operability in high data applications. LoRaWAN has a wider band of 125, 150 or 500 kHz and allows adaptive data rates in a range of 10 kbps and payloads of max 57 bytes/message. Thus, the provided data rates by NB-IoT and CAT-M1 are higher than those given by LoRaWAN and Sigfox, especially in downlink transmission, which makes NB-IoT and CAT-M1 is better in case of the IoT applications are in need of high downlink data rate.

Property/ Technology	**NB-IoT**	**LoRaWAN**	**Sigfox**	**LTE-M (CAT-M1)**
Spectrum [MHz]	700-900 3 Depl. Modes	Europe 868,433 US 915 Asia 430	Europe 868 US 902 Asia 923	700-900 In-band
Duty cycle	100 %	Europe: 1% US: non	Europe: 1% US: non	100%
Bandwidth [kHz]	3GPP 200 standalone 180 in-band	US 500-250-125 Europa 250-125	192 kHz	1.4 MHz
Data rate [bps]	67k UL 30k DL	0.3 – 50 k ADR Different for DL	100 or 600	< 1 Mbps
Payload Per message		57 bytes	12 bytes max.	

Table 3.1. Comparison of Technologies on Critical Features

3.3. Power consumption and Coverage

NB-IoT and CAT-M1 are legacy wireless networks and are standardized by 3GPP which targets to minimize the power consumption and achieve battery lifetime that lasts for 10 years at least. The power consumption is directly related to other important properties including long-range coverage, downlink transmission, maximum allowed payload. These features play a vital role in deciding the domain of technology usage. Table 3.2 shows the battery lifetime (5 Wh) of different LPWA technologies on average coverage (MCL = 150 dB) and medium payload (50 bytes/2 hours**) .** Furthermore, NB-IoT achieves wider coverage than CAT-M1, with a range of 15 km and 11 km respectively. Both technologies use QPSK and OFDM technologies following the R13 3GPP standard. That offers less complexity into the physical layer than GSM/LTE.

On the other hand, Sigfox and LoRaWAN technologies achieved 13 km and 11km of coverage [8], respectively. Coverage area is related to the signal propagation channel. Maximum coupling Loss (MCL) values of all technologies are shown in Table 3.2 as a measure of coverage given by each technology. All technologies achieve full coverage in outdoor environments. However, better indoor coverage is achieved by NB-IoT and Sigfox than LoRa with 1% outage capacity for NB-IoT and 2% outage capacity for LoRaWAN in case of 20 dB indoor loss. For 30 dB penetration loss such as a basement or thick concrete wall environments, NB-IoT offers 8% outage capacity, Sigfox 13% and LoRa 20%. That makes NB-IoT and CAT-M1 ideal technologies for deep indoor coverage, whereas LoRaWAN is ideal for rural areas where 3G/4G coverage is not available because of the deployment of independent gateways. Sigfox on the other hand, follows the same operator model as 3G/4G and can set up more base stations depending on the customer's needs.

The key to long coverage of each technology is the physical layer but some conditions limit the performance. For example, transmitted power in Sigfox and LoRa is affected by regional limitations (14 dBm for LoRa and 14-27dBm for Sigfox) [6]. NB-IoT and CAT-M1 support transmitted signal of 23 dBm. The comparison between these two groups from coverage perspective is kind of unfair, but however in advantage for NB-IoT and CAT-M1. LoRa and Sigfox overcome these challenges in different ways to still be able to compete as a potential candidate for long-range industrial IoT services. LoRa deploys chirp spread spectrum as modulation which performs on large distances and is robust against interference and noise, while Sigfox uses Ultra Narrow Band with slow modulation scheme BPSK.

All technologies afford lifetime battery of ten years at least, sometimes in the cost of range, but in general the long-range requirement is satisfied. The suitability for industrial networks depends on the deployment area of application. In case of the applications are in need of deep indoor coverage, then CAT-M1 is the best choice, otherwise, LoRa can serve well for long range rural environments.

Property/ Technology	**NB-IoT**	**LoRaWAN**	**Sigfox**	**LTE-M (CAT-M1)**
Power consumption	11 years	13 years	13 years	10 years
Range MCL Outdoor Indoor 20 dB loss Indoor 30 dB loss	15 km 164 dB Full 1% outage capacity 8%	<11 156 dB Full 2% outage capacity 20%	<13 km 160 dB Full 1% outage capacity 13%	<11 km 156 dB Full Full Full
Transmitted power	23 dBm	14 dBm	14-27 dBm	23 dBm
Physical Layer	QPSK Sectorized one antenna	CSS Omni-directional one antenna	BPSK + UNB Omni-directional one antenna	16 QAM Sectorized antenna

Table 3.2. Coverage Comparison

3.4. Quality of Service

All technologies under our focus deploy different mechanisms to offer high quality of service but NB-IoT and CAT-M1 have a great advantage over LoRaWAN and Sigfox because of using licensed spectrum. That advantage is at the expense of cost though. Moreover, NB-IoT and Cat-M1 support a high quality of service by increasing retransmission times which increase the coverage and QoS. In LoRaWAN and Sigfox, the connection with multiple gateways makes the network to choose the best message in terms of quality among all messages received by gateways which is their method to obtain a good QoS. Sigfox utilizes three types of diversity to hold the quality of service needed for IoT services including spatial diversity, frequency diversity, and time diversity. Table 3.3 includes the QoS of the technologies [8].

3.5. Latency

Latency is the time delay from making a transmission request until the time that packets are actually transmitted from the end-devices to the base stations. Data in IoT services are not transmitted immediately because this consumes battery fast and decreases the coverage area. From this aspect, NB-IoT and CAT-M1 are considered to be low latency technologies due to regular synchronization with the network which is infrequent though. CAT-M1 offers latency in millisecond whereas NB-IoT offers between 6 - 10 sec latency. In contrast to legacy cellular technologies, LoRaWAN and Sigfox use medium access technology based on Aloha protocol which is an asynchronous protocol and provides high or medium latency for services. In industrial LPWA networks, for applications that are sensitive to delay or real-time applications that need to act immediately if an event occurs, CAT-M1 and NB-IoT are better to implement, outranking Sigfox and LoRaWAN high-latency performances [8].

Property/ Technology	**NB-IoT**	**LoRaWAN**	**Sigfox**	**LTE-M (CAT-M1)**
QoS	Very High	High	high	Very high
Latency	medium	medium	medium	low
Mobility	No	Yes Non-GPS	Yes Non-GPS	Full GPS-based

Table 3.3. QoS, Latency and Mobility Comparison

3.6. Mobility

CAT-M1 supports complete mobility for end-nodes through frequent synchronization with the base station. But NB-IoT, surprisingly, [10] offers no support for mobility in connected-state devices. Devices should go to idle mode, then make a handover to another cell and then return to connected mode again. LoRaWAN and Sigfox support full mobility because of the connectivity to multiple gateways. If an end-node is moving, it is the duty of network to choose the best signal from one gateway and therefore no handover is needed. That makes them better suited for transportation-type applications. LoRaWAN and Sigfox geolocation depends on gateways and not on GPS which offers non-accurate low-power location services. In contrast, CAT-M1 is GPS-based providing accurate high-power location services.

3.7. Cost

In general, all IoT technologies are classified as low-cost with less than 10$ for cost per module. However, it is not only a module cost to be taken into account. Different cost aspects are taken in consideration in the following subsections.

3.7.1 Module Cost

As shown in Table 3.4, module cost in LoRaWAN and Sigfox is lower than NB-IoT and CAT-M1 due to the fact that higher complexity requires more cost. However, in the continuously growing IoT market, the prices of modules will most likely converge. Some electronics manufacturers have already designed and introduced some hybrid solutions for IoT (all technologies in one chip) for medium prices per module. Module complexity varies according to the technology. As a comparison between CAT-M1 and NB-IoT, the module is more complex in CAT-M1 (mobility, larger bandwidth, higher data rates, voice traffic is supported) and that fact increases modem complexity and cost as a consequence which makes NB-IoT to have an advantage over CAT-M1 from the perspective of cost. Modem complexity is even less in LoRaWAN and Sigfox because of lower bandwidth, slower modulation technique, less coding complexity, low downlink transmission and security requirements [22].

3.7.2 Network Cost

There are two categories as far as IoT networks are concerned, including vendor-managed networks as LoRaWAN and operator-managed networks such as Sigfox, NB-IoT and CAT-M1. These technologies are quite new and quickly changing. What is supposed to be a standard today, can be out of date in a few years and that is why it is very important to make intelligent choices about network infrastructure.

The cost of the network in vendor-managed networks depends on whether private network or public network is used. Some cities offer public

LoRaWAN-based network for free, but in industrial IoT, private network should be deployed for higher reliability and security. The cost of network deployment in Sigfox is less than the cost in NB-IoT because of the cost caused by the data traffic when using cellular technologies which is estimated to reach 3-5 $/month for 1MB of data traffic in CAT-M1 and less than 1 $ for NB-IoT [22].

Firmware over the air is allowed in all technologies but Sigfox which is an additional advantage for these technologies to save upgrading costs in the long run.

Property/ Technology	**NB-IoT**	**LoRaWAN**	**Sigfox**	**LTE-M (CAT-M1)**
module price	10- 15 $	9- 12$	5- 10 $	7- 12 $
modem complexity	15 % compared to 3GPP, RE8	-	-	20 % compared to 3GPP, RE8
duplex mode multiplexing peak DL	half duplex yes / no 170 kbps	no non 30 kbps	no non 40 bps	half duplex yes 1 Mbps
connectivity	1 $/ month /100 kB	free in public 500 $ construction	< 1 $ / month	3- 5 $/mon /1 MB
FoTA	yes	yes	no	yes

Table 3.4 Module cost

3.7.3 Availability

Availability of technology in the targeted locations is considered to be an important measure of the ability to use the technology, since finding the right operator is essential for long-term cost savings. In Figure 3.1 [23] the coverage offered by Sigfox in Sweden and Denmark is given, and it is clear that not whole Sweden is covered by Sigfox which makes knowing the availability of technology in a target location, a critical key point for the success of future projects. On the other hand, in cellular systems, the coverage is still under roll-out in many countries as shown in Figure 3.2 [24].

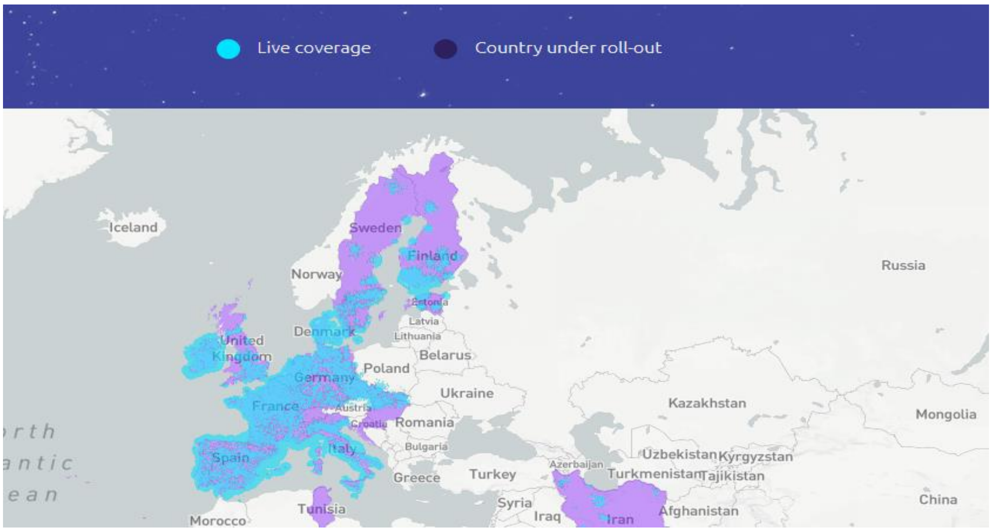

Figure 3.1. Sigfox Coverage Map

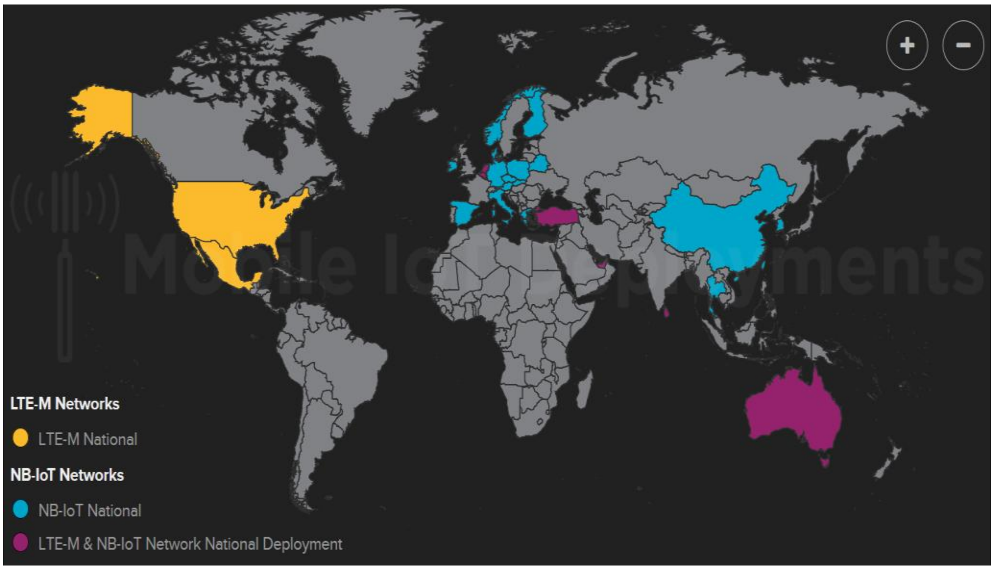

Figure 3.2. NB-IoT and CAT-M1 Coverage Map

3.8. Applications

In conclusion, the suitability of specific technology in industrial LPWA networks depends on the needs of specific industrial applications. Every specific application in industrial IoT that provides its user with specific services requires different features from the technology that provides the connectivity. Some of the applications are introduced here to find the best technical solution.

3.8.1. Smart Metering Applications

Smart metering applications seem to be future for metering solutions since it is estimated that already 700 million smart metering devices are used worldwide, 50% of them in China [25]. Smart meters usually transmit a small amount of data (uplink data size of 10 bytes) containing parameters related to the service. For instance, in water metering or gas metering applications, sensors transmit water consumption or gas level measurements few times during the day. Weather metering applications are used to transmit temperature and humidity data with relatively large time intervals.

These types of applications require that the radio technology has a large capacity (thousands of connected devices), low power consumption in end-devices, support large range and very low cost in order to deploy a large number of devices per customer.

LoRaWAN can be considered to be a suitable choice for most such applications assuming that the cost of gateway installation is reasonable. Sigfox as well, serves adequately for these applications as long as the data payload is limited to 12 bytes. In other cases when high data throughput is needed, NB-IoT and CAT-M1 are better choices [26].

3.8.2 Network Monitoring Applications

These applications contain network-command and software upgrading services. Network-command services are used, in addition to metering and reporting objectives, for start-up and shut-down purposes which require a medium data size in the downlink (at least 12 bytes per hour or day). Regarding software upgrading services, the requirements of downlink data is up to 1000 bytes per hour or day.

NB-IoT is the best choice for applications that require from an hour to one-day transmission cycles and relatively large downlink data size. LoRaWAN and Sigfox are out of range of such applications because of their low size of downlink transmission and of the limitations on duty cycle [10].

3.8.3. Applications in Manufacturing Sector

Control over types of machinery, industrial automation and other services within the manufacturing sector vary depending on their specific requirements. When industrial services demand more frequent, bidirectional transmission and confirmed QoS, NB-IoT and CAT-M1 are best choices for these applications. NB-IoT and CAT-M1 enable features of more frequent transmission and very high reliability. CAT-M1 fits best when high data rates and low latency for industry scenarios are needed. LoRaWAN and Sigfox are less probable to serve in the manufacturing sector.

3.8.4. Supply Chain Tracking Applications

Regarding transportation applications where moving or in-storage objects are tracked, the requirement that should be fulfilled is a good performance on mobility with low power consumption. Suitable technologies are LoRaWAN, Sigfox, and CAT-M1. The choice of LoRaWAN and Sigfox is because of the connection to multiple gateways that allows them to perform reliably on moving assets where no high data rate is required [26]. CAT-M1 also supports mobility and tracking scenarios using its advantage of deep-indoor coverage [27].

3.8.5. Agriculture Applications

These applications involve the transmission of the agriculture indicators, such as water consumption, soil state, and temperature data. These services do not require an instant response (downlink transmission) or very frequent data transmission. In this case, Sigfox or LoRaWAN can be suitable radio technologies to provide connectivity for these applications.

3.8.6. Power Generator Monitoring

This application is used by HMS company. The services applied by this application include monitoring the state of power generator and metering the diesel tank level. This power generator is stationary, and it sends two types of data, including scheduled data and event-driven data. Scheduled data includes fuel level, battery level, engine status and temperature. This data payload can be more or less on demand of the operator and transmitted four times per hour. Event-driven data is alarm when the fuel level is low, or when the engine's temperature is high.

The requirements of power Generator are high coverage for stationary objects distributed in outdoor urban or rural area. Data payload up to 30 bytes and transmitted in 15 minutes time interval, or event-driven data to be transmitted in reasonable delay of few minutes. High reliability is required as well.

LoRaWAN can be considered to be a suitable choice for this application. Sigfox as well, serves adequately here as long as the data payload is limited. NB-IoT is better choice than both LoRaWAN and Sigfox because NB-IoT can transmit more frequently and reliably and has a higher payload in the downlink.

Chapter 4. Practical Implementation

4.1. Selection Approach

4.1.1. Introduction

It has been explained and shown in the comparison section that there is not a singular solution for the vast variety of Industrial IoT applications. However, depending on the very specific characteristics of each application and on the needs of the customer, some technologies are more suitable than others. In the second section, two categories were introduced including proprietary technologies (Sigfox and LoRaWAN) and non-proprietary technologies (NB-IoT and CAT-M1). Proprietary technologies are usually more suitable for the majority of the Industrial IoT applications due to the fact that they provide long-range coverage in combination with low power consumption, unlicensed bandwidth usage, robustness against interference, reasonable latency, adjustment in real time applications, mobility and localization. The main advantages of this branch of technologies are cost-effectiveness and flexibility in network design because of the ability to construct a private network consisting its own gateways and its own cloud server which can be connected to application servers based on customers' requirements. This offers the capability to deploy the technology in rural areas where there is no need of pre-existing network beforehand. One important thing to take in consideration during the deployment of proprietary technologies, is the regulations regarding the usage of frequency bands and transmitted power. These limitations do not affect the usage negatively but require some modifications on the data transmission such as being able to transmit six messages per hour due to duty cycle 1% and setting 14dBm as maximum transmitted power. Under this restriction, Sigfox and LoRaWAN are considered to be more cost-efficient and energy-saving solutions for the majority of Industrial IoT applications.

4.1.2. Choosing Sigfox

There were two different paths for the direction regarding the selection of the most suitable technology, described as follow:

1. To design our own network from scratch with all equipment, which is considered as costly and time consuming as far as the time scale of our project was concerned. Besides, that path should contain work and duties out of the scope of our study, such as programming a mobile application to monitor the functionality of modules, programming the gateway to work as needed which requires found knowledge of computer science.

2. To use existing network infrastructure that is ready to be utilized by devices and prototypes. However, following this path, challenges still exist to understand the used programs to extract the information we need in our test. Sigfox affords a complete backhaul (availability of gateway in main cities of Sweden) and cloud-based server that provide users with various useful characteristics of the module such as Signal to Noise Ratio (SNR), Received Signal Strength Indicator (RSSI), Delay, and Frequency bands. That is why Sigfox is classified as Operator-Managed Network. On the other hand, LoRaWAN is classified as Vendor-Managed Network, i.e. vendor are totally responsible for the network design and construction. Fortunately, Lund City provides, through its project "Future by Lund" an open city sensor network to be publicly used by interested researchers, students and other who are interested to experiment and develop new solutions in pre-commercial stage [28]. These facilities encouraged us to follow this path, having into our disposal existing networks.

The selection of the technology that we used in the practical implementation, was based initially on the availability of the technologies in the area of Sweden and specifically in Lund and Malmö. During the starting phase of the project, it was realised quite fast that NB-IoT and CAT-M1 could not be used because of their premature deployment in the area. Therefore, in order to avoid complications and finish the project according to the schedule, we decided to test the performance of Sigfox and LoRaWAN since all the required resources were more accessible (module and integration to the network). The Pycom module [29] that was used for the measurement procedure is being presented in the Equipment Overview section of the thesis. The main reason we concluded in ordering this specific module, was that it could support both Sigfox and LoRaWAN technologies. In addition to that, Pycom module can be programmed in microPython. Code can be found in Appendix A.

At first, we came into contact with Future by Lund [28]. The gateway in Lund in combination with the rest of the network infrastructure proved to have a poor and unpromising performance at the time. We were unable to conduct a reasonable amount of measurements due to the lack of reliability of the service. This is the reason why we performed test scenarios only for Sigfox regarding the scope of this thesis. Sigfox offers a fixed network with gateways that have stable performance over time and can lead to successful measurements and meaningful results. Consequently, our only need was to obtain the Pycom module and program it in order to begin the practical implementation stage.

4.2 Measurement Methodology

4.2.1 Equipment Overview

The growing IoT market, in the recent years, due to the increasing need for IoT devices, offers the users and industrial factories with a large variation of devices to support all different needs. For the purpose of this thesis, a Pycom module, Lopy4 [29] was used during the measurement process. Lopy4 enables the utilization of four technologies in one chip (WI-FI, LoRa, Sigfox, BLE). According to its specifications [29], transmit power is equal to 14 dBm, optimized for power efficiency and operates within the SRD860 frequency band. After it is connected to an expansion board, Lopy4 can be easily programmed using microPython. In order to set up the module a boot.py file is needed to be configured. In order to start transmitting through the medium, a main.py file must be modified accordingly. In our case, we configured the module to transmit 6 bytes every 2 minutes (6 minutes for one case). In Appendix A.1, a case of transmission every 2 minute is shown. The respective codes that were used for the purpose of this thesis, are given in Appendix A. To protect the chipset, we put the composite module in a protecting case, called Pycase. The antenna used is dipole antenna with 2 dBi gain. The choice of this kind of antenna is based on simplicity. The composite module is shown on Figure 4.1.

Figure 4.1. Pycom module used for measurements

In order to modify the *boot.py* and *main.py* files, a file transfer protocol (FTP) connection has to be established. In addition, in order to be able to use the module running on Sigfox, registration on Sigfox's portal needs to be made, followed by a Device ID and PAC Number. More detailed information about the set-up and software installation of the module can be found in [29].

4.2.2 Scenarios Overview

The main core of the measurement methodology of this thesis is to study the coverage, suitability for real time application in terms of delay and latency, and reliability in terms of corrupted and missed messages during the transmission of Sigfox technology in the areas of Lund and Malmö, consisting of rural, urban, indoor and outdoor topologies. We use the existing network infrastructure of Sigfox. The locations are selected in such a way to depict different cases of signal propagation and path loss, including outdoor and indoor locations with different penetration losses in both rural and urban areas. In some scenarios, we test also the coverage for moving end-devices. The coverage is examined using the path loss parameter as a measure of the range obtained by the technology. The end-device that is used, operates at 868 MHz and is equipped with an omni-directional antenna of 2 dBi gain. The transmission power is given in chapter 2 to be equal to 14 dBm. The heights of Lund and Malmö base stations are equal to 94 and 63 meters respectively with respect to the ground level (AGL). The module is mounted on different heights at the locations which serves additional food for thought and analysis. In Table 4.1, the various scenarios are being shown, including the calculated distance from the main two base stations in Lund and Malmö and also including characteristics of each scenario. Complete measurement data can be given after request to the authors.

Measurement Set	Distance from Base Station (m)	Height of Module (m)	Scenario Tested
No. 1	500	1	Indoor, Urban
No. 2	2.37 k	1	Outdoor, Urban
No. 3	2.54 k	2.5	Outdoor, Urban
No. 4	2.54 k	1.5	Outdoor, Urban
No. 5	2.44 k	1	Indoor, Urban
No.6	14 k	1.5	Outdoor, Rural
No. 7	1.72 k	3	Indoor, Urban
No. 8	1.72 k	3	Indoor, Urban
No. 9	75	1	Outdoor, Urban
No. 10	4.5 k	1	Outdoor, Urban
No. 11	4.5 k	1	Indoor Dense Urban
No. 12	500	1	Indoor, Urban

No. 13	5.5 k	1	Outdoor Suburban
No. 14	4.5-5.5 k	2	Moving, Rural
No. 15	6 k	6	Indoor, Rural
No. 16	6 k	6	Outdoor, Rural
No. 17	3 -10 k	2	Rural, Moving
No. 18	5- 8 k	2	Urban, Moving
No. 19	10 k	2	Rural, Outdoor

Table 4.1. Scenarios Tested

The locations are pointed in the maps, as Figure 4.2-4 are shown, in Lund, Malmö and Hurva. The locations are numbered to be consistent with Table 4.1. The yellow pointer refers to the base stations, the red ones to the module's locations and the green ones to point the module when moving.

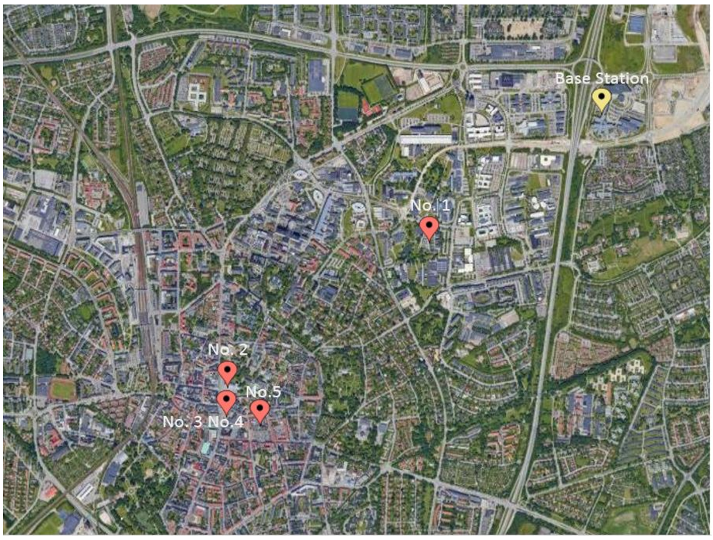

Figure 4.2. Locations in Lund

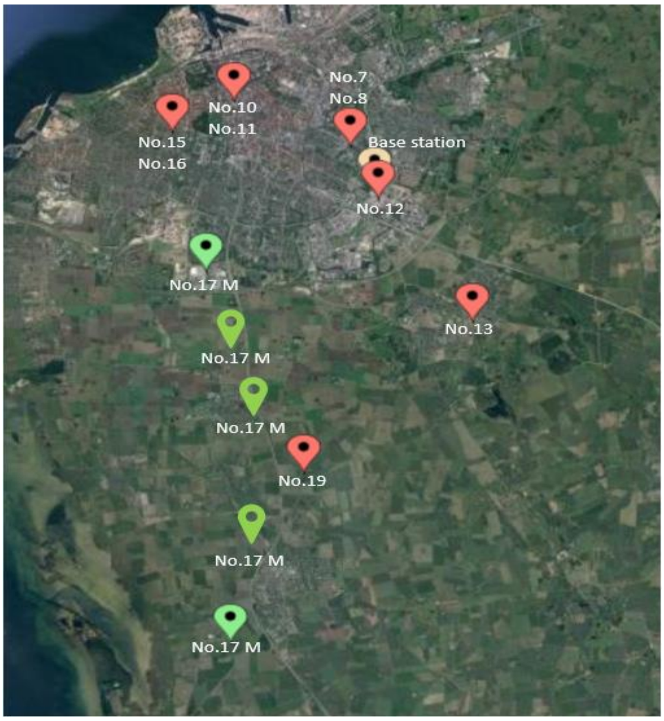

Figure 4.3. Locations in Malmö

Figure 4.4. Location in Hurva

4.3 Results

Table 4.2 shows the results extracted from each measurement set as far as each scenario is concerned. These results include statistical parameters that are important for the analysis of the technology's performance, such as: average path loss, average latency, outage capacity and average RSSI. The values in Table 4.2 come from further processing of the measurement set tables we get from Sigfox backend.

Latency is a very important metric that influences radically real-time applications. In our case, it is the combination of time on air and the delay for the message to be transmitted from the base station to the backend server. The time on air is two seconds for each message which means that six seconds are needed for three packets which are transmitted by Sigfox over three different frequencies. The delay that is shown at the Sigfox backend is the time between reception of message on the base station and reception by backend depending on backhaul connectivity (Ethernet, 3G, 4G). Therefore, in order to compute the end-to-end latency, 6 seconds have to added to each delay. The mean value of each measurement set delays gives the average latency as shown in Table 4.2. The remaining metrics provide useful information regarding the coverage and reliability of the technology within the different scenarios. Outage capacity is calculated as the percentage of the messages that were not delivered or received at any base station. Average RSSI is equal to the mean value of the RSSI values for each measurement set. Path loss (or equally coupling loss) comes from a link budget calculation given as follows on (3):

$$path\ loss = transmitted\ power + antenna\ gain - RSSI \qquad (3)$$

where *transmitted power* refers to the module's radiated power, which is equal to 14 dBm according to module specifications, *antenna gain* is equal to 2 dBi and $RSSI$ is extracted from the measurement sets. The mean value of the path loss from each measurement set is the average path loss.

Measurement Set	Average Path Loss(dB)	Average Latency(s)	Outage Capacity(%)	Average RSSI (dBm)
No. 1	141.826	7.62	65	-125.826
No. 2	146	7.49	62.5	-130
No. 3	145.034	7.44	27.5	-129.034
No. 4	144.762	7.47	47.5	-128.762
No. 5	139.129	7.6	22.5	-123.129
No. 6	133.533	7.43	0	-117.533
No. 7	116.25	7.4875	0	-100.2500
No. 8	123.7333	7.65	0	-107.7333
No. 9	88.30	7.395	0	-72.3000 R
No. 10	134.2308	7.5503	0	-118.2308
No. 11	144.1875	7.6074	62.79	-128.1875
No. 12	105.6970	7.4419	0	-89.6970
No .13	135.2188	7.4530	6.15	-119.2188
No. 14	124.8750	7.8118	0	-108.87
No. 15	144.0645	7.3621	45.45	-128.0645
No. 16	132.9714	7.3718	0	-116.9714
No. 17	133.6667	7.3252	0	-117.6667
No. 18	88.3333	8.2350	30	-72.3333
No. 19	132.6207	7.7667	0	-116.6207

Table 4.2. Measurement Results

Regarding the measurements in Malmö, the results of outdoor scenarios, No.9, No.10, No.14, No.16 and No.19, whether rural area or urban area, show full reliability as long as the device is mounted as high as possible, i.e. no message have been missed in outdoor cases, No.9 the module is located in outdoor near to the base station and the received signal is considered reference signal, in No. 10 the module is located outdoor in dense area with people and transportation in Triangeln, in No. 16 the module is located outdoor in suburban area near to Stadion, in No.19 the module is located outdoor in urban area in Vellinge. On the other hand, indoor cases provide different outage probability in service, which results in unreliability of services in indoor cases. Sigfox is better to be used in rural areas or where a line of sight is available between base stations and end-devices. In a special case of outdoor scenario such as No.13, the module is mounted outdoor 5km away from the base station, in the middle of a suburban area surrounded completely by high buildings that obstruct the line of sight connection with the base station. This scenario shows loss of connection equal to 6 %.

Indoor scenario with 30 dB penetration loss in No.11, results in high outage probability equal to 60.2%. In this scenario, the module is located about 4.5 km far away from the base station in a shopping mall (Triangeln) which is dense with people and transportation around. Another indoor scenario, No. 13 with 10 dB loss shows less outage probability than the previous one even though the module is located 5.5 km more distant from the base station. That leads to the fact that the main factor to be taken into consideration to achieve high reliability is the environment there the module is located.

As far as the movement is considered, it is noticed from measurements that moving end-devices in No.14 have a good performance (Latency of 6-7 seconds and full coverage within 13 km range) but the environment has, as we studied in few lines above, the main impact on the reliability. That is noticed clearly from the measurement No. 17 of moving module with speed of 90 km/h on distance between 4-10 km from the base station through rural area, the outage probability is less than 1% which result in excellent reliability in Sigfox for moving objects in rural areas. But again in urban areas the reliability decreases in our moving module as measurements in No.18 show that we get 30% outage in the connectivity during the moving through the city.

The latency or the maximum time to get the signal received and processed at the backend server is between 6-9 seconds in most of the cases. This latency is considered reasonable to make Sigfox a usable technology in real time applications, if the limited downlink capacity is taken into consideration.

As far as Lund is concerned, two indoor scenarios were performed as shown in Table 4.1. No.1 took place deep inside E-huset building at Lund University which is just 500 meters away from the base station in Lund. No.2 took place close to window surface in the center, with a distance equal to 2.44 kilometers. It is quite interesting, that No.2, even if its distance is about 5 times higher than No.1, it provides better overall performance and about 3 times increased reliability. This can be attributed to the deep penetration losses that are added when the module is placed in deep indoor scenarios. In cases where it is close to a window, such as No.5, it provides almost same performance as in outdoor scenarios. On the other hand, 3 outdoor urban scenarios were performed in the center of Lund with a distance of 2.37-2.54 kilometers from the base station. No.3 took place behind Lund Cathedral which has a height equal to 55 meters. The height of the module was 1 meter and because of the massive obstacle of the Cathedral, poor performance was expected. Average RSSI of this measurement set was the worst compared to the other sets. Outage capacity was high, almost equal to No.1 which shows that shadowing caused by the large object can cause severe signal attenuation and corruption in the communication channel. In order to verify that, No. 3 scenario took place about 150-200 meters away from No.2, facing again Lund Cathedral as an obstacle towards the base station. The key difference in this scenario was the height of the module which was set to be equal to 2.5 meters. As expected, outage capacity was reduced by less than half in approximate which verifies the negative effect of shadowing on No.2. No.4 is in the same location as No.3, but the height of the module is set to 1.5 meters. RSSI values are following the same pattern but outage capacity is increased again up to 47.5%. This increase can be attributed to the different height of the module. The higher the transmitting device is located, the better performance and reliability can be assured.

The maximum coverage that was experienced, was up to 14 km in the area of Hurva, and that proves that Sigfox can actually reach 14 km range. Outdoor coverage up to 5 km range can easily be achieved by Sigfox with good signal to noise ratio (SNR) and good Received Signal Strength Indicator RSSI.

Chapter 5. Conclusion

In this master thesis, a theoretical analysis of the most prominent LPWAN technologies for Industrial IoT is pursued in Chapter 2. Sigfox, LoRaWAN, CAT-M1 and NB-IoT are analysed in terms of technical features, network infrastructure and security. In Chapter 3, a theoretical comparison regarding bandwidth, data rate, power consumption, coverage, quality of service, latency, mobility and cost is provided and based on that, the different technologies are being assigned as more suitable for specific industrial IoT applications.

As far as the practical part is concerned, Sigfox was chosen as the test technology for the scope of this work. Both indoor, outdoor, rural and urban scenarios were examined in the area of Skåne (Lund, Hurva and Malmö). Measured parameters include received signal strength indicator (RSSI), signal to noise ratio (SNR), delay and link quality. Further processing of these values leaded to useful metrics such as average path loss, average SNR, average latency and average RSSI for each measurement set and examined scenario.

It was shown that for indoor scenarios, signal attenuation was noticed which was an expected result. Sigfox radio technology does not operate optimally in deep indoor topologies where lots of walls and doors are included. The most intense case of this phenomenon was noticed in location No.1 where outage capacity reached its maximum value of 65%. However, it reaches almost outdoor performance if the module is placed in an area with windows. For outdoor scenarios, and specifically urban, Malmö's cases showed optimal reliability with outage capacity less than 1%. However, in the area of Lund, for the same type of scenarios, outage capacity reached very high values with a peak equal to 62.5%, which can be attributed to the topology including high buildings and obstacles between the module and the base station (shadowing effect). As far as coverage is concerned, the measurement set in Hurva, showed that Sigfox can support transmissions up to 14 km. Testing mobility inside a car showed full outdoor capacity. However, when the module is outside the moving object, outage capacity drops below 6%.

As a conclusion, regarding the application that motivated us to start this thesis work, which is the Diesel tank monitoring application, Sigfox proved to live up to our expectations due to its good overall reliability and coverage performance. Monitoring of diesel tanks does not require a heavy data payload (needs to transmit only the level of the oil). Therefore 6 bytes per message, that we used for our measurements, satisfy this requirement. As far as latency is concerned, diesel tank monitoring does not require real-time updates, therefore 7-9 seconds of overall delay as shown in our measurements, do not affect this type of application. Regarding coverage, Sigfox performs optimally in outdoor scenarios providing low values of outage capacity. In indoor cases, Sigfox proves to be insufficient but for this type of applications, the module will unlikely ever be placed in indoor environments. However, the specific topology has always to be taken into serious consideration since high buildings and obstacles in general, have a negative effect on communication. Furthermore, our measurements verify that Sigfox can reach 14 km, given that the module is placed in a rural environment with free space between itself and the base station.

This type of application, due to its low data payload and no need for real-time notifications/updates, can be supported also by LoRaWAN. LoRaWAN technology, provides companies with the capability of setting up their own private network, which can turn out to be much more cost efficient and secure in the long run. NB-IoT and CAT-M1 are also suitable technologies for this kind of application. However, their increased cost and decreased lifetime can only be justified when there is need for higher data payload.

Chapter 6. Future Work

Future work includes testing the remaining technologies that have been studied theoretically, such as LoRaWAN, CAT-M1 and NB-IoT. This will provide the companies with more detailed information about the applications that can properly be served by one of these technologies.

For comparison purposes, that can be done in the same locations and scenarios as those which are used in this work. This will allow to study the interference in each technology that is produced by the legacy wireless connections in NB-IoT, and by adjacent wireless connections and other devices in unlicensed frequency bands in SRD868 or ISM bands for LoRaWAN and Sigfox.

Some Future work is intended to be in action by NB-IoT team in [7] to find out the network model that characterizes the operability of NB-IoT networks. That work will deepen the interest in a more detailed link budget of NB-IoT which is different from the existing 3G/4G link budget analysis.

References

[1] U. Raza, P. Kulkarni and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855-873, Second quarter 2017.

[2] G. Margelis, R. Piechocki, D. Kaleshi and P. Thomas, "Low Throughput Networks for the IoT: Lessons learned from industrial implementations," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 181-186.

[3] Margaret Rouse, September 2017, "LPWAN (Low Power Wide Area Network)",[http://internetofthingsagenda.techtarget.com/definition/LPWAN-low-power-wide-area-network], accessed April 2018.

[4] HMS company labs associated with Netbiter, 2016, "Diesel Tank Monitoring",[https://www.netbiter.com/applications/power-generators-ups/diesel-tank-monitoring], accessed May 2018.

[5] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen and M. Sorensen, "Interference Impact on Coverage and Capacity for Low Power Wide Area IoT Networks," 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, 2017, pp. 1-6.

[6] Benny Vejlgaard, Mads Lauridsen, Huan Nguyen, Istvan Z. Kovacs, Preben Mogensen, Mads Sorensen, "Coverage and Capacity Analysis of Sigfox Lora GPRS and NB-IoT", Vehicular Technology Conference (VTC Spring) 2017 IEEE 85th, pp. 1-5, 2017.

[7] M. Chen, Y. Miao, Y. Hao and K. Hwang, "Narrow Band Internet of Things," in IEEE Access, vol. 5, pp. 20557-20577, 2017.

[8] SUNHA, R., WEI, Y., HWANG, S., 2017, "A Survey on LPWA technology: LoRa and NB-IoT", Information and communication Technology Express.

[9] Sigfox official website [https://www.sigfox.com/en], accessed 2018-04-24.

[10] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi and S. He, "Narrowband Internet of Things: Implementations and Applications," in IEEE Internet of Things Journal, vol. 4, no. 6, pp. 2309-2314, Dec. 2017.

[11] K. E. Nolan, W. Guibene and M. Y. Kelly, "An evaluation of low power wide area network technologies for the Internet of Things," 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, 2016, pp. 439-444.

[12] LoRa Alliance Technical Marketing Workgroup, November 2015, "A technical Overview of LoRa and LoRaWAN"

[13] B. Reynders and S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," 2016 Symposium on Communications and Vehicular Technologies (SCVT), Mons, 2016, pp. 1-5.

[14] Mick Mack, Apr 2, 2017, "LoRaWAN on Batteries, how long does it last",[https://www.mickmake.com/post/lora-on-batteries-how-long-does-it-last-technology], accessed April 2018.

[15] LoRa Alliance Technical Committee LoRaWAN, October 11, 2017. LoRaWAN 1.1 Specification.

[16] P. Neumann, J. Montavont and T. Noël, "Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study," 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, 2016, pp. 1-8.

[17] Sacha Kavanagh, 2018, "What is Narrowband IoT?", [https://5g.co.uk/guides/what-is-narrowband-iot/], accessed April 2018.

[18] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul and A. Ghosh, "LTE-M Evolution Towards 5G Massive MTC," 2017 IEEE Globecom Workshops (GC Wkshps), Singapore, 2017, pp. 1-6.

[19] Brain ray in Link Labs, Maj 2017, available online [https://www.link-labs.com/blog/what-is-lte-m], accessed April 2018.

[20] Glenn Schatz in Link Labs, November 2017, webinar available online [https://www.youtube.com/watch?v=07AYeg_eu7w], accessed April 2018.

[21] A. Díaz-Zayas, C. A. García-Pérez, Á. M. Recio-Pérez and P. Merino, "3GPP Standards to Deliver LTE Connectivity for IoT," 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, 2016, pp. 283-288.

[22] Jian Hua Wu. 14-06-2017. “NB-IoT Technical Fundamentals”.

[23] Sigfox.May-2015. online [https://www.sigfox.com/en/coverage], accessed 16 May 2018.

[24] GSMA deployment map, available online [https://www.gsma.com/iot/deployment-map/], accessed 16 May 2018.

[25] Philippe Garnier. 13-february 2017. available online [https://blog.sigfox.com/is-2017-the-year-of-the-smart-meter/] . accessed may 2018.

[26] Art Reed. 14 july 2017. available online [http://www.bluesignal.com/2017/07/13/nb-iot-vs-lora-its-an-ecosystem-not-a-race/] accessed 16-05-2018.

[27] Nokia Networks white paper, “LTE-M – Optimizing LTE for the Internet of Things”, available online[https://novotech.com/docs/default-source/default-document-library/lte-m-optimizing-lte-for-the-internet-of-things.pdf?sfvrsn=0], accessed in May 2018.

[28] Future by Lund, Open City Sensor network. Available online [http://www.futurebylund.se/locsn-en], accessed in May 2018.

[29] Pycom [https://pycom.io/hardware/lopy4-specs/], accessed May 2018.

[30] the things network group. available online [https://www.thethingsnetwork.org/docs/lorawan/security.html]. accessed 2018-06-06.

Appendix A

A.1 Main.py

```
from network import Sigfox
import socket
import time

# init Sigfox for RCZ1 (Europe)
sigfox = Sigfox(mode=Sigfox.SIGFOX, rcz=Sigfox.RCZ1)

# create a Sigfox socket
s = socket.socket(socket.AF_SIGFOX, socket.SOCK_RAW)

# make the socket blocking
s.setblocking(True)

# configure it as uplink only
s.setsockopt(socket.SOL_SIGFOX, socket.SO_RX, False)

# send some bytes
while True:
    s.send(bytes([1, 2 ,3 , 4, 5, 6]))
    time.sleep(120)
```

A.2 Boot.py

```
from machine import UART
import machine
import os

uart = UART(0, baudrate=115200)
os.dupterm(uart)
machine.main('main.py')
```

Printed by Tryckeriet i E-huset, Lund 2018

Lund University

Series of Master's theses
Department of Electrical and Information Technology
LU/LTH-EIT 2018-645
http://www.eit.lth.se